บทที่ 7

ยูนิคแฟคเตอร์ไรเซชันโดเมน

(Unique Factorization Domain)

ในบทที่จะศึกษาเรื่องยูนิคแฟคเตอร์ไรเซชันโดเมน ซึ่งกล่าวถึงการแยกตัวประกอบของสมาชิกในอินทิกรัลโดเมน และการแยกตัวประกอบของโพลิโนเมียลบนฟิลด์

7.1. ปรินซิปัลไอดีลโดเมน (Principal Ideal Domain)

นิยาม 7.1.1 ให้ R เป็นคอมมิวเททีฟริง ที่มียูนิตี้ ถ้า N เป็นไอดีลของ R และ

$N = (a) = \{ra \,/\, r \in R\}$ สำหรับ $a \in R$ จะเรียก N ว่าเป็นปรินซิปัลไอดีล (principal ideal)

ตัวอย่าง 7.1.1 พิจารณาริง I ซึ่งเป็นคอมมิวเททีฟริงที่มียูนิตี้ และ

$$N = (3) = \{3r \,/\, r \in I\}$$
$$= \{\ldots -6, -3, 0, 3, 6, \ldots\ldots\}$$

จะได้ว่า N เป็นปรินซิปัลไอดีลของ I

นิยาม 7.1.2 ให้ D เป็นอินทิกรัลโดเมน จะกล่าวว่า D เป็นปรินซิปัลไอดีลโดเมน (Principal Ideal Domain) ถ้าทุกๆไอดีลของ D เป็นปรินซิปัลไอดีล

สัญลักษณ์ จะเขียน PID แทนปรินซิปัลไอดีลโดเมน

ข้อสังเกต จากทฤษฎี 6.3.1 ได้ว่าทุกๆยูคลิเดียนโดเมนเป็น PID

<u>ตัวอย่าง 7.1.3</u> อินติกรัลโดเมน I เป็น PID

<u>นิยาม 7.1.3</u> ให้ p เป็นสมาชิกของอินติกรัลโดเมน D โดยที่ $p \neq 0$ และ p ไม่ใช่ยูนิตจะเรียก p ว่าเป็นสมาชิกเฉพาะ (irreducible) ของ D ถ้า $p = ab$ ซึ่ง $a, b \in D$ โดยที่ a หรือ b ตัวใดตัวหนึ่งจะต้องเป็นยูนิต

หรือกล่าวได้ว่า p จะเป็นสมาชิกเฉพาะในอินติกรัลโดเมน D ก็ต่อเมื่อ p แยกตัวประกอบได้เป็นผลคูณของสมาชิกสัมพันธ์ของ p และยูนิตใน D เท่านั้น

<u>ข้อสังเกตุ</u> สมมุติว่า p เป็นสมาชิกเฉพาะดังนั้น $p = qu$ เมื่อ u คือยูนิตในอินติกรัลโดเมน D จากนิยาม 6.1.3 แสดงว่า p และ q เป็นสมาชิกสัมพันธ์ และจาก $p = qu$ ทำให้ $pu^{-1} = q$ แสดงว่า q แยกตัวประกอบได้เป็นผลคูณของ p ซึ่งไม่ใช่ยูนิต แต่เป็นสมาชิกสัมพันธ์ของ q กับ u^{-1} ซึ่งเป็นยูนิตใน D นั่นคือ q เป็นสมาชิกเฉพาะ

ดังนั้น ถ้า p เป็นสมาชิกเฉพาะแล้ว จะได้ว่าสมาชิกสัมพันธ์ของ p จะเป็นสมาชิกเฉพาะด้วย

<u>ตัวอย่าง 7.1.4</u> พิจารณาอินติกรัลโดเมน I ซึ่งมี 1 และ −1 เป็นยูนิต จะพบว่า 7 เป็นสมาชิกเฉพาะของ I เพราะว่า $7 = (1)(7)$ หรือ $7 = (-1)(-7)$

<u>ทฤษฎี 7.1.1</u> ให้ D เป็น PID และ (p) เป็นไอดีลของ D แล้วจะได้ว่า (p) เป็นแม็กซิมัลไอดีลของ D ก็ต่อเมื่อ p เป็นสมาชิกเฉพาะใน D

<u>พิสูจน์</u> <u>ตอนแรก</u> สมมุติให้ (p) เป็นแม็กซิมัลไอดีลของ PID แล้วจะพิสูจน์ว่า p เป็นสมาชิกเฉพาะใน D

สมมุติว่า p ไม่เป็นสมาชิกเฉพาะ นั่นคือ $p = ab$ โดยที่ $a, b \in D$ และทั้ง

a , b ไม่เป็นยูนิต

จะได้ว่า $(ab) \subsetneq (a)$

นั่นคือ $(p) \subsetneq (a)$

สมมุติ $(a) = (p)$

ดังนั้นจะมี $x \in D$ ซึ่ง $a = px$

นั่นคือ $a = (ab)x$

หรือ $ae = a(bx)$

โดยอาศัยกฎการตัดออกสำหรับการคูณ จะได้ว่า

$$e = bx$$

แสดงว่ามี $x \in D$ ซึ่งทำให้ $bx = e$

นั่นคือ b เป็นยูนิตใน D ซึ่งขัดแย้งกับที่ว่า b ไม่เป็นยูนิตใน D

ดังนั้น $(p) \neq (a)$

เนื่องจาก (p) เป็นแม็กซิมัลไอดีล ดังนั้นจะได้ว่า $(a) = D$

นั่นคือ $(a) = (e)$

ดังนั้นจะมี $y \in D$ ซึ่ง $ay = e$

นั่นคือ a เป็นยูนิตใน D ซึ่งขัดแย้งกับที่ว่า a ไม่เป็นยูนิตใน D

แสดงว่า ถ้า $p = ab$ แล้วจะได้ว่า a หรือ b จะต้องเป็นยูนิตใน D

นั่นคือ p เป็นสมาชิกเฉพาะ

<u>ตอนสอง</u> สมมุติให้ p เป็นสมาชิกเฉพาะใน D แล้วจะพิสูจน์ว่า (p) เป็นแม็กซิมัลไอดีลของ D

ถ้าให้ $(p) \subsetneq (a) \subseteq D$ เมื่อ $a \in D$ ....(1)

ดังนั้น สมาชิกใน (p) เขียนเป็นผลคูณของ a ได้

นั่นคือ $p = ab$ สำหรับบางสมาชิก $b \in D$

ถ้า a เป็นยูนิตใน D ดังนั้นจะมี $a^{-1} \varepsilon D$

และเนื่องจาก (a) เป็นไอดีลใน D

ดังนั้น $aa^{-1} = e \varepsilon (a)$

จากทฤษฎี 4.1.1 จะได้ว่า (a) = D

ถ้า a ไม่เป็นยูนิต แล้ว b จะต้องเป็นยูนิต

นั่นคือ มี $x \varepsilon D$ ซึ่ง $bx = e$

เนื่องจาก $p = ab$

ดังนั้น
$$\begin{aligned} px &= (ab)x \\ &= a(bx) \\ &= a.e = a \end{aligned}$$

นั่นคือ $(a) \subseteq (p)$ ....(2)

จาก ....(1) และ ...(2) จะได้ว่า (a) = (p)

เนื่องจาก $(p) \neq D$ และถ้า $(p) \subseteq (a)$ แล้วพิสูจน์ได้ว่า (a) = D

หรือ (a) = (p) อย่างใดอย่างหนึ่ง

นั่นคือ (p) เป็นแม็กซิมัลไอดีลใน D

__ทฤษฎี 7.1.2__ ให้ D เป็น PID ถ้า p เป็นสมาชิกเฉพาะใน D และ p / ab

เมื่อ $a , b \varepsilon D$ แล้วจะได้ว่า p/a หรือ p/b

__พิสูจน์__ เนื่องจาก p / ab เมื่อ $a , b \varepsilon D$

ดังนั้น $ab = px$ สำหรับ $x \varepsilon D$

นั่นคือ $ab \varepsilon (p)$

จากทฤษฎี 7.1.1 ได้ว่า (p) เป็นแม็กซิมัลไอดีลของ D

และจากทฤษฎี 4.4.2 ได้ว่า (p) เป็นไอดีลเฉพาะของ D

ดังนั้น $a \in (p)$ หรือ $b \in (p)$

นั่นคือ $a = pu$ หรือ $b = pv$ สำหรับ $u, v \in D$

แสดงว่า p / a หรือ p / b

<u>บทแทรก 7.1.3</u> ให้ D เป็น PID ถ้า p เป็นสมาชิกเฉพาะใน D และ p หาร ผลคูณ $a_1 a_2 \ldots\ldots a_n$ สำหรับ $a_i \in D$ ได้ลงตัว แล้วจะได้ว่ามี i อย่างน้อยตัวหนึ่งที่ทำให้ p / a_i

<u>พิสูจน์</u> แบบฝึกหัด

7.2. <u>ยูนิคแฟคเตอร์ไรเซชันโดเมน</u> (Unique Factorization Domain)

<u>นิยาม 7.2.1</u> ให้ D เป็นอินทิกรัลโดเมน จะเรียก D ว่าเป็นยูนิคแฟคเตอร์ไรเซชันโดเมน ถ้า D สอดคล้องคุณสมบัติต่อไปนี้

1. สมาชิกทุกตัวของ D ที่ไม่ใช่ศูนย์และไม่เป็นยูนิต สามารถที่จะแยกตัวประกอบได้เป็นผลคูณของสมาชิกเฉพาะที่มีจำนวนจำกัด

2. ถ้าสมาชิกของ D_r สามารถแยกตัวประกอบได้ 2 ชุด คือ $p_1 \ldots\ldots p_r$ และ $q_1 \ldots\ldots q_s$ โดยที่ p_i และ q_i ต่างเป็นสมาชิกเฉพาะ แล้วจะได้ว่า $r = s$ และสามารถเปลี่ยนตำแหน่ง q_i เพื่อทำให้ p_i และ q_i เป็นสมาชิกสัมพันธ์กันได้

<u>สัญลักษณ์</u> เขียน UFD แทน ยูนิคแฟคเตอร์ไรเซชันโดเมน

<u>ตัวอย่าง 7.2.1</u> อินทิกรัลโดเมน I เป็น UFD เพราะว่าทุกๆสมาชิกใน I สอดคล้องนิยาม 7.2.1 เช่น $24 \in I$ จะได้

$$24 = (2)(2)(3)(2)$$

และ

$$24 = (-2)(-3)(2)(2)$$

ซึ่ง 2 กับ −2 และ 3 กับ −3 เป็นสมาชิกสัมพันธ์
จะเห็นว่าถ้ายกเว้นเรื่องลำดับ (order) และการสัมพันธ์กันแล้ว ตัวประกอบซึ่งเป็นสมาชิกเฉพาะของ 24 ทั้ง 2 ชุดนี้ เหมือนกัน

<u>เล็มมา 7.2.1</u> ให้ D เป็น PID ถ้า $\{N_i\}$ เมื่อ $i = 1,2,\ldots\ldots$ เป็นอันดับ (sequence) ของไอดีลของ D ที่มีจำนวนไม่จำกัด ซึ่งสอดคล้อง

$N_1 \subsetneq N_2 \subsetneq \cdots \subseteq N_i \subsetneq N_{i+1} \subsetneq \cdots\cdots$ แล้วจะมีจำนวนเต็มบวก r ซึ่ง

$N_r = N_s$ สำหรับทุกๆ $s \geq r$

<u>พิสูจน์</u> เนื่องจาก $N_1 \subseteq N_2 \subseteq \cdots\cdots\cdots$ สำหรับไอดีล N_i ใน D

ให้ $N = \bigcup_i N_i$

ดังนั้น $N \subsetneq D$ และ $N \neq \emptyset$

จะแสดงว่า N เป็นไอดีลของ D

สมมุติให้ $a, b \in N$

ดังนั้นจะมีไอดีล N_{i_1} และ N_{i_2} ซึ่ง $a \in N_{i_1}$ และ $b \in N_{i_2}$

และ $N_{i_1} \subseteq N_{i_2}$ หรือ $N_{i_2} \subsetneq N_{i_1}$

สมมุติว่า $N_{i_1} \subsetneq N_{i_2}$ ดังนั้นทั้ง a และ b อยู่ใน N_{i_2}

เนื่องจาก N_{i_2} เป็นไอดีลของ D

ดังนั้น $a - b$ และ $ab \in N_{i_2}$

นั่นคือ $a - b$ และ $ab \in N$

แสดงว่า N เป็นสับริงของ D

ให้ $a \in N$ และ $d \in D$

นั่นคือ $a \in N_{i_1}$ สำหรับบาง N_{i_1}

เนื่องจาก N_{i_1} เป็นไอดีลของ D ดังนั้นจะได้ $da = ad$ อยู่ใน N_{i_1}

นั่นคือ $ad = da \in \bigcup_i N_i$ หรือ $ad = da \in N$

ดังนั้น N เป็นไอดีลของ D

เนื่องจาก D เป็น PID ดังนั้นจะได้ว่า $N = (c)$ สำหรับ $c \in D$

และเนื่องจาก $N = \bigcup_i N_i$ ดังนั้นจะได้ว่า $c \in N_r$ สำหรับบาง $r \in I^+$

สำหรับ $s \geq r$ จะได้ว่า

$$(c) \subseteq N \subsetneq N_s \subseteq N = (c)$$

นั่นคือ $N_r = N_s$ สำหรับ $s \geq r$

<u>ทฤษฎี 7.2.2</u> ให้ D เป็น PID ทุกๆสมาชิกที่ไม่เป็นศูนย์ และไม่ใช่ยูนิตใน D จะเขียนเป็นผลคูณของสมาชิกเฉพาะได้

<u>พิสูจน์</u> ให้ $a \in D$ เมื่อ $a \neq 0$ และ a ไม่เป็นยูนิต

จะต้องแสดงว่า a จะมีตัวคูณร่วมที่เป็นสมาชิกเฉพาะอย่างน้อยหนึ่งตัว

ถ้า a เป็นสมาชิกเฉพาะ จะได้ว่าทฤษฎีเป็นจริง

ถ้า a ไม่เป็นสมาชิกเฉพาะ นั่นคือ $a = a_1b_1$ เมื่อ a_1 และ b_1 ไม่เป็นยูนิตใน D

ดังนั้น $(a) \subsetneq (a_1)$

ถ้า $(a) = (a_1)$ จะได้ว่า $a_1 = va$ สำหรับบางสมาชิก $v \in D$

ดังนั้น $a_1 = v(a_1b_1)$

$a_1e = a_1(vb_1)$

จะได้ $e = vb_1$

แสดงว่า b_1 เป็นยูนิตใน D ซึ่งจะขัดแย้งกับที่ให้ b_1 ไม่เป็นยูนิต

ดังนั้น $(a) \neq (a_1)$ นั่นคือ $(a) \subset (a_1)$

โดยวิธีเดียวกันนี้ ต่อไปเริ่มต้นด้วย a_1 จะได้ว่า $(a_1) \subset (a_2)$ ทำเช่นนี้ไปเรื่อยๆ จะได้ว่า

$$(a) \subset (a_1) \subset (a_2) \subset \ldots\ldots$$

โดยอาศัยเล็มม่า 7.2.1 จะได้ว่า chain ของไอดีลนี้จะต้องสิ้นสุดที่ (a_r)

สำหรับบาง a_r และ a_r จะต้องเป็นสมาชิกเฉพาะ นั่นคือ a มี a_r เป็นตัวคูณร่วมที่เป็นสมาชิกเฉพาะ

จากที่พิสูจน์มาแล้วนี้ จะเห็นว่าสำหรับสมาชิก $a \neq 0 \in D$ และ a ไม่ใช่ยูนิต ใน D

จะได้ว่า a เป็นสมาชิกเฉพาะ หรือ $a = p_1c_1$ โดยที่ p_1 เป็นสมาชิกเฉพาะ

และ c_1 ไม่ใช่ยูนิต

โดยทำนองเดียวกันกับการพิสูจน์ข้างต้น จะได้ว่าในกรณีที่ $a = p_1c_1$

ทำให้ได้ว่า $(a) \subset (c_1)$

ถ้า c_1 ไม่ใช่สมาชิกเฉพาะ จะได้ $c_1 = p_2c_2$ โดยที่ p_2 เป็นสมาชิกเฉพาะ

และ c_2 ไม่ใช่ยูนิต

ทำเช่นนี้ไปเรื่อยๆจะได้ chain ของไอดีล

$$(a) \subset (c_1) \subset (c_2) \subset \ldots\ldots\ldots$$

จากเล็มม่า 7.2.1 chain ของไอดีลนี้จะต้องสิ้นสุดที่บาง $c_r = q_r$ ซึ่งเป็นสมาชิกเฉพาะ

ดังนั้น $$a = p_1p_2 \cdots p_rq_r$$

นั่นคือ a เขียนเป็นผลคูณของสมาชิกเฉพาะได้

<u>ทฤษฎี 7.2.3</u> ทุกๆ PID เป็น UFD

<u>พิสูจน์</u> ให้ D เป็น PID และ $a \in D$ เมื่อ $a \neq 0$ และ a ไม่ใช่ยูนิต

โดยทฤษฎี 7.2.2 จะได้ว่า $a = p_1p_2 \cdots p_r$ เมื่อ p_i เป็นสมาชิกเฉพาะ สำหรับ $i = 1, \ldots, r$

จะต้องแสดงว่า a เป็นผลคูณของสมาชิกเฉพาะได้แบบเดียวเท่านั้น

สมมุติว่า a สามารถเขียนเป็นผลคูณของสมาชิกเฉพาะได้อีกแบบหนึ่งคือ

$$a = q_1q_2 \cdots q_s \quad \text{เมื่อ } q_j \text{ เป็นสมาชิกเฉพาะสำหรับ } j = 1, \ldots, s$$

เนื่องจาก p_1 / a ดังนั้นจะได้ว่า $p_1 / (q_1q_2 \cdots q_s)$

จากบทแทรก 7.1.3 จะได้ว่า p_1 / q_{j_1} สำหรับบาง j_1 ซึ่ง $1 \leq j_1 \leq s$

สมมุติให้ $j_1 = 1$

ดังนั้นจะได้ p_1 / q_1

นั่นคือ $q_1 = p_1u_1$ สำหรับ $u_1 \in D$

เนื่องจาก p_1, q_1 เป็นสมาชิกเฉพาะ ดังนั้น u_1 เป็นยูนิต

แสดงว่า p_1 และ q_1 เป็นสมาชิกสัมพันธ์

ดังนั้น จะได้ $p_1p_2 \cdots\cdots p_r = p_1u_1q_2 \cdots\cdots q_s$

โดยอาศัยกฎการตัดออกสำหรับการคูณใน D จะได้

$$p_2 \cdots\cdots p_r = u_1q_2 \cdots\cdots q_s$$

โดยวิธีการเดียวกันโดยเริ่มที่ p_2 ทำไปเรื่อยๆในที่สุดจะได้

$$e = u_1u_2 \cdots\cdots u_rq_{r+1} \cdots\cdots q_s$$

โดยที่ u_i, $i = 1, 2, \cdots\cdots r$ เป็นยูนิต

เนื่องจาก q_j เป็นสมาชิกเฉพาะ ดังนั้นจะได้ $r = s$

แสดงว่า PID เป็น UFD

<u>บทแทรก 7.2.4</u> (Fundamental Theorem of Arithmatics)

อินติกรัลโดเมน I เป็น UFD

<u>พิสูจน์</u> เนื่องจากทุกๆไอดีลใน I เขียนได้เป็น $(n) = \{nr \,/\, r \in I\}$

สำหรับ $n \in I$

แสดงว่า I เป็น PID

จากทฤษฎี 7.2.3 จะได้ว่า I เป็น UFD

<u>แบบฝึกหัด 7 ก</u>

1. จงพิสูจน์บทแทรก 7.1.3
2. จงบอกว่าสมาชิกในแต่ละอินทิกรัลโดเมน ที่กำหนดให้ต่อไปนี้ อันใดเป็นสมาชิกเฉพาะ

   ก. 5 ใน I ข. -17 ใน I

   ค. 14 ใน I ง. $2x - 3$ ใน $I[x]$

   จ. $2x - 10$ ใน $I[x]$ ฉ. $2x - 3$ ใน $Q[x]$
3. จงแสดงว่าใน PID ทุกๆไอดีลจะอยู่ในแม็กซิมัลไอดีล
4. กำหนดให้ I, J, K เป็นไอดีลของ PID , R , จงแสดงว่าความสัมพันธ์ต่อไปนี้เป็นจริง

   ก. ถ้า $I = (a)$ และ $J = (b)$ แล้ว $IJ = (a)$ และ $I^n = (a^n)$

   ข. $I(J \cap K) = IJ \cap IK$

   ค. $I + (J \cap K) = (I + J) \cap (I + K)$

   ง. $I \cap (J + K) = (I \cap J) + (I \cap K)$

   จ. $IJ = I \cap J$ ก็ต่อเมื่อ $I + J = R$ สำหรับทุกๆค่าของ $I \neq 0$, $J \neq 0$
5. จงแสดงว่าสมาชิก 2 ตัวใดๆ ที่ไม่ใช่ศูนย์ของ UFD จะมี ห.ร.ม.

   [Hint : ถ้า $a = p_1^{k_1} p_2^{k_2} \cdots\cdot p_r^{k_r}$ และ $b = p_1^{l_1} p_2^{l_2} \cdots\cdots p_r^{l_r}$

   (p_i เป็นสมาชิกเฉพาะแล้ว $(a , b) = p_1^{j_1} p_2^{j_2} \cdots\cdot p_r^{j_r}$, ซึ่ง

   $j_i = \min (k_i, l_i)$]
6. จงแสดงว่าริงของจำนวนตรรกยะ m/n ซึ่ง n เป็นจำนวนคี่เป็น PID

7.3. การแยกตัวประกอบของโพลิโนเมี่ยลบนฟิลด์

(Facterization of Polynomials over Field)

7.3.1 ดิวิชันอัลกอริทึมใน $F[x]$ (Division Alforithm in $F[X]$)

ในบทที่ 3 ได้กล่าวถึงโพลิโนเมี่ยลริง $R[x]$ มาแล้ว สำหรับในหัวข้อนี้จะกล่าวถึงการแยกตัวประกอบของสมาชิก $f(x)$ ใน $F[x]$ เมื่อ F เป็นฟิลด์

ทฤษฎีที่จะกล่าวถึงต่อไปนี้เป็นดิวิชันอัลกอริทึมใน $F[x]$ ซึ่งคล้ายกับดิวิชันอัลกอริทึมใน I

__ทฤษฎี 7.3.1.1__ ให้ $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots\cdots + a_o$ และ

$g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_o$ เป็นสมาชิกใน $F[x]$ เมื่อทั้ง a_n และ b_m เป็นสมาชิกที่ไม่ใช่ศูนย์ใน F และ $m > 0$ จะได้ว่ามีโพลิโนเมี่ยล $q(x)$ และ $r(x)$ เพียงอย่างละตัวใน $F(x)$ ที่ทำให้ $f(x) = g(x)q(x) + r(x)$, โดยที่ดีกรีของ $r(x)$ น้อยกว่าดีกรีของ $g(x)$ ซึ่งเท่ากับ m

__พิสูจน์__ พิจารณาเซ็ท $S = \{f(x) - g(x)s(x) \;/\; s(x) \in F[x]\}$

ให้ $r(x)$ เป็นสมาชิกใน S ที่มีดีกรีน้อยที่สุด

ดังนั้นจะได้ $r(x) = f(x) - g(x)q(x)$ สำหรับบาง $q(x) \in F[x]$

นั่นคือ $f(x) = g(x)q(x) + r(x)$

จะต้องแสดงว่าดีกรีของ $r(x)$ น้อยกว่า m

สมมุติว่า $r(x) = c_tx^t + c_{t-1}x^{t-1} + \cdots + c_o$ เมื่อ $c_i \in F$ และ $c_t \neq 0$

ถ้า $t \neq 0$

ถ้า $t \geq m$

ดังนั้น $\left[f(x) - q(x)g(x) \right] - \left(\frac{c_t}{b_m} \right)x^{t-m} g(x) = r(x) - \left(\frac{c_t}{b_m} \right)x^{t-m}g(x)$ ..(1)

พิจารณา $r(x) - \left(\frac{c_t}{b_m} \right)x^{t-m} g(x) = (c_t x^t + c_{t-1}x^{t-1} + \cdots + c_o) - \left(\frac{c_t}{b_m}\right)x^{t-m}(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_o)$

$$= (c_t x^t + c_{t-1}x^{t-1} + \cdots + c_o) - \left(c_t x^t + \frac{c_t b_{m-1}}{b_m} x^{t-1} + \cdots + \frac{c_t b_o}{b_m} x^{t-m}\right)$$

$$= \left(c_{t-1} - \frac{c_t b_{m-1}}{b_m}\right)x^{t-1} + \cdots + c_o$$

ซึ่งเป็นโพลิโนเมี่ยลของ x ที่มีดีกรีน้อยกว่า t

เนื่องจากโพลิโนเมี่ยลทางซ้ายของ .... (1) เขียนได้เป็น

$$f(x) - g(x)\left[q(x) + \left(\frac{c_t}{b_m} \right) x^{t-m} \right]$$

ดังนั้น $f(x) - g(x)\left[q(x) + \left(\frac{c_t}{b_m} \right)x^{t-m}\right] \varepsilon S$ และมีดีกรีน้อยกว่า t

ซึ่งจะขัดแย้งกับที่ให้ $r(x) \varepsilon S$ โดยที่ $r(x)$ มีดีกรีน้อยที่สุดคือ t

นั่นคือ $t \geq m$ ไม่ได้ แสดงว่า $t < m$ หรือดีกรีของ $r(x)$ น้อยกว่าดีกรีของ $g(x)$

ต่อไปจะแสดงว่า $q(x)$ และ $r(x)$ มีเพียงอย่างละตัว

สมมุติให้ $f(x) = g(x)q_1(x) + r_1(x)$ โดยที่ดีกรี $r_1(x)$ < ดีกรี $g(x)$

และ $f(x) = g(x)q_2(x) + r_2(x)$ โดยที่ดีกรี $r_2(x)$ < ดีกรี $g(x)$

จะได้ $0 = g(x)[q_1(x) - q_2(x)] + [r_1(x) - r_2(x)]$ . .

หรือ $g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x)$ ......(2)

เนื่องจากดีกรีของ $r_2(x) - r_1(x)$ น้อยกว่าดีกรี $g(x)$

ดังนั้น ..(2) จะเป็นจริง เมื่อ $q_1(x) - q_2(x) = 0$

นั่นคือ $q_1(x) = q_2(x)$

ซึ่งทำให้ได้ว่า $r_2(x) - r_1(x) = 0$

ดังนั้น $r_2(x) = r_1(x)$

<u>ตัวอย่าง 7.3.1.1</u> ให้ $f(x)$ และ $g(x)$ เป็นสมาชิกใน $I_5[x]$ โดยที่

$f(x) = x^4 - \bar{3}x^3 + \bar{2}x^2 + \bar{4}x - \bar{1}$ และ $g(x) = x^2 - \bar{2}x + \bar{3}$

จะหา $q(x)$ และ $r(x)$ ในทฤษฎี 7.3.1.1 โดยการหาร $f(x)$ ด้วย $g(x)$ คำนวณได้โดยการใช้วิธีหารยาว

$$
\begin{array}{r|l}
 & x^2 - x - \bar{3} \\
\hline
x^2 - \bar{2}x + \bar{3} & x^4 - \bar{3}x^3 + \bar{2}x^2 + \bar{4}x - \bar{1} \\
 & \underline{x^4 - \bar{2}x^3 + \bar{3}x^2} \\
 & \quad - x^3 - x^2 + \bar{4}x \\
 & \quad \underline{- x^3 + \bar{2}x^2 - \bar{3}x} \\
 & \qquad - \bar{3}x^2 + \bar{2}x - \bar{1} \\
 & \qquad \underline{- \bar{3}x^2 + x - \bar{4}} \\
 & \qquad\qquad x + \bar{3}
\end{array}
$$

<u>นิยาม 7.3.1.1</u> ให้ a เป็นสมาชิกในฟิลด์ F จะเรียกว่า a เป็นราก (root) ของ $f(x) \in F[x]$ ก็ต่อเมื่อ $x - a$ เป็นตัวประกอบของ $f(x)$ ใน $F(x)$

<u>บทแทรก 7.3.1.2</u> ให้ $f(x)$ เป็นโพลิโนเมียลดีกรี $n > 0$ ของ $F(x)$ จะได้ว่า $f(x)$ จะมีรากที่แตกต่างกันในฟิลด์ F ได้อย่างมากที่สุด n ราก

<u>พิสูจน์</u> ถ้า a_1 เป็นรากของ $f(x)$ โดยที่ $a_1 \in F$

ดังนั้น $f(x) = (x - a_1)q_1(x)$ เมื่อ $q_1(x) \in F[x]$

เนื่องจาก $f(x)$ มีดรกรี n ดังนั้น $q_1(x)$ จะมีดีกรี $n - 1$

ให้ a_2 เป็นรากของ $q_1(x)$ เมื่อ $a_2 \in F$

ดังนั้น $f(x) = (x - a_1)(x - a_2)q_2(x)$ เมื่อ $q_2(x) \in F[x]$

โดยวิธีการเดียวกันนี้จะได้

$$f(x) = (x - a_1)(x - a_2) \dots (x - a\ )q_r(x)$$

เมื่อ $q_r(x) \in F[x]$ และ $q_r(x)$ ไม่มีรากใน F , เห็นได้ชัดว่า $r \leq n$

และถ้า $b \neq a_i$ สำหรับ $i = 1,2,\dots, r$ และ $b \in F$

ดังนั้น $f(b) = (b - a_1)(b - a_2) \dots (b - a_r)q_r(b)$

เนื่องจาก F ไม่มีตัวหารศูนย์ และทั้ง $b - a_i$ และ $q_r(b)$ ไม่เท่ากับศูนย์

ดังนั้น $f(b) \neq 0$

นั่นคือ a_i ทั้งหมด สำหรับ $i = 1, \dots, \leq n$ เป็นรากของ $f(x)$ และ $a_i \in F$

7.3.2 <u>โพลิโนเมี่ยลเฉพาะ</u> (Irreducible Polynomial)

<u>นิยาม 7.3.2.1</u> ให้ $f(x) \in F(x)$ โดยที่ $f(x)$ ไม่เป็นโพลิโนเมี่ยลค่าคงที่จะเรียกว่า $f(x)$ เป็นโพลิโนเมี่ยลเฉพาะใน $F(x)$ ถ้า $f(x)$ ไม่สามารถเขียนเป็นผลคูณของ $g(x)h(x)$ เมื่อ $g(x)$ และ $h(x)$ เป็นสมาชิกใน $F(x)$ ซึ่งทั้ง $g(x)$ และ $h(x)$ มีดีกรีเป็นบวก และน้อยกว่าดีกรีของ $f(x)$

<u>ตัวอย่าง 7.3.2.1</u> ให้ $x^2 - 2$ เป็นสมาชิกในโพลิโนเมี่ยลริง $\mathbb{R}(x)$ จะได้ว่า $x^2 - 2$ ไม่เป็นโพลิโนเมี่ยลเฉพาะใน $\mathbb{R}(x)$ เนื่องจากสามารถแยกตัวประกอบของ $x^2 - 2$ ได้เป็น $(x - \sqrt{2})(x + \sqrt{2})$

<u>ตัวอย่าง 7.3.2.2</u> ให้ $x^2 + 1$ เป็นสมาชิกในโพลิโนเมี่ยลริง $\mathbb{R}(x)$ จะได้ว่า $x^2 + 1$ เป็นโพลโนเมี่ยลเฉพาะ แต่ถ้าให้ $x^2 + 1 \in C(x)$ แล้ว $x^2 + 1$ จะไม่เป็นโพลิโนเมี่ยลเฉพาะ เนื่องจาก $x^2 + 1 = (x + i)(x - i)$ เมื่อ $i = \sqrt{-1}$

<u>ตัวอย่าง 7.3.2.3</u> ให้ $f(x) = x^3 - \bar{3}x + \bar{2}$ เป็นสมาชิกในโพลิโนเมี่ยลจริง $I_5(x)$

สมมุติว่า $f(x) = x^3 + \bar{3}x + \bar{2}$ แยกตัวประกอบได้ใน $I_5(x)$

นั่นคือ $x^3 + \bar{3}x + \bar{2} = (x - a)g(x)$ เมื่อ $g(x) \in I_5(x)$ และ $g(x)$ มีดีกรีน้อยกว่า 3, $a \in I_5$

จากนิยาม 7.3.1.1 จะได้ว่า a เป็นรากของ $f(x)$

พิจารณา $f(0) = 2$, $f(1) = 1$, $f(-1) = -2$, $f(2) = 1$ และ $f(-2) = -2$

แสดงว่า $f(x)$ ไม่มีรากที่อยู่ใน I_5

ดังนั้น $x^3 + \bar{3}x + \bar{2}$ แยกตัวประกอบไม่ได้ใน $I_5(x)$

นั่นคือ $x^3 + \bar{3}x + \bar{2}$ เป็นโพลิโนเมียลเฉพาะใน $I_5(x)$

<u>ทฤษฎี 7.3.2.1</u> ถ้า F เป็นฟิลด์แล้วทุกๆไอดีลของ $F(x)$ จะเป็นปรินซิปัลไอดีล

<u>พิสูจน์</u> ให้ N เป็นไอดีลของ $F(x)$

ถ้า $N = \{0\}$ เมื่อ 0 คือ โพลิโนเมียลศูนย์ใน $F(x)$

จะได้ $N = (0)$ เมื่อ 0 คือ สมาชิกศูนย์ใน F

$= \{0 \cdot f(x) \,/\, f(x) \in F(x)\}$

ถ้า $N \neq \{0\}$

ให้ $g(x)$ เป็นสมาชิกของ N โดยที่ $g(x)$ ไม่เป็นโพลิโนเมียลศูนย์ และมีดีกรีน้อยที่สุด

ถ้าดรกรีของ $g(x)$ เป็น 0, ดังนั้น $g(x) \in F$

เนื่องจากทุกๆ สมาชิกใน F มีอินเวอร์สสำหรับการคูณ

จะได้ว่า $g(x)$ เป็นยูนิทใน F

ดังนั้นจะได้ $N = F(x)$

นั่นคือ $N = (e)$ เมื่อ e คือยูนิตี้ใน F

ถ้าดีกรีของ $g(x) \geq 1$

ให้ $f(x)$ เป็นสมาชิกใดๆใน N จากทฤษฎี 7.3.1.1 จะได้ว่ามี $q(x)$, $r(x) \in F(x)$ ที่ทำให้

$f(x) = g(x)q(x) + r(x)$ โดยที่ดีกรีของ $r(x) <$ ดีกรีของ $g(x)$

เนื่องจาก N เป็นไอดีล และ $f(x)$, $g(x) \varepsilon N$

ดังนั้น $f(x) - g(x)q(x) \varepsilon N$

นั่นคือ $r(x) \varepsilon N$

เนื่องจาก $g(x)$ เป็นสมาชิกใน N ที่มีดีกรีน้อยที่สุด และ $g(x)$ ไม่เป็นโพลิโนเมี่ยลศูนย์

ดังนั้น $r(x) = 0$

นั่นคือ $f(x) = g(x)\ q(x)$ สำหรับ $q(x) \varepsilon F[x]$

แสดงว่า $N = (g(x))$

นั่นคือ N เป็นปรินซิปัลไอดีลใน $F(x)$

ทฤษฎี 7.3.2.2 ให้ $(p(x))$ เป็นไอดีลใน $F(x)$ เมื่อ $p(x)$ ไม่ใช่โพลิโนเมี่ยลศูนย์ แล้วจะได้ว่า $(p(x))$ เป็นแม็กซิมัลไอดีลของ $F(x)$ ก็ต่อเมื่อ $p(x)$ เป็นโพลิโนเมี่ยลเฉพาะใน $F(x)$

พิสูจน์ ตอนแรก สมมุติว่า $(p(x))$ เป็นแม็กซิมัลไอดีลของ $F(x)$ โดยที่ $(p(x)) \neq \{0\}$ เมื่อ 0 คือ โพลิโนเมี่ยล

เนื่องจาก $(p(x)) \neq F(x)$ แสดงว่า $p(x) \notin F$

สมมุติ $p(x)$ ไม่เป็นสมาชิกเฉพาะใน $F(x)$

นั่นคือ $p(x)$ แยกเป็นผลคูณของ 2 โพลิโนเมี่ยลที่มีดีกรีน้อยกว่าดีกรีของ $p(x)$ และไม่เท่ากับศูนย์ได้ดังนี้

$$p(x) = f(x)g(x) \qquad \text{..........(1)}$$

เนื่องจาก $(p(x))$ เป็นแม็กซิมัลไอดีล และจากทฤษฎี 4.4.2 จะได้ว่า $(p(x))$ เป็นไอดีลเฉพาะ

จากนิยาม 4.4.2 จะได้

$$f(x) \varepsilon (p(x)) \qquad \text{หรือ} \qquad g(x) \varepsilon (p(x))$$

นั่นคือ $f(x)$ เขียนเป็นผลคูณของ $p(x)$ ได้ หรือ $g(x)$ เขียนเป็นผลคูณของ $p(x)$ ได้

แสดงว่าดีกรีของ $p(x)$ น้อยกว่าดีกรีของ $f(x)$ หรือ ดีกรีของ $p(x)$ น้อยกว่าดีกรีของ $g(x)$ ซึ่งจะขัดแย้งกับ .... (1)

นั่นคือ $p(x)$ เป็นโพลิโนเมียลเฉพาะใน $F[x]$

<u>ตอนสอง</u> สมมุติให้ $p(x)$ เป็นโพลิโนเมียลเฉพาะใน $F[x]$

สมมุติว่า N เป็นไอดีลของ $F[x]$ ซึ่ง $(p(x)) \subseteq N \subseteq F[x]$

จากทฤษฎี 7.3.2.1 ได้ว่า N เป็นปรินซิปัลไอดีล

ดังนั้น $N = (g(x))$ สำหรับบาง $g(x) \in F[x]$

เนื่องจาก $(p(x)) \subseteq N \subseteq (g(x))$

ดังนั้น $p(x) \in (g(x))$

แสดงว่า $p(x) = g(x)\,q(x)$ สำหรับบาง $q(x) \in F[x]$

แต่ $p(x)$ เป็นโพลิโนเมียลเฉพาะใน $F(x)$

ดังนั้น $g(x)$ หรือ $q(x)$ จะต้องมีดีกรี 0

ถ้า $g(x)$ มีดีกรี 0

นั่นคือ $g(x) = a$, $a \in F$ และ $a \neq 0$

แสดงว่า $g(x)$ เป็นยูนิตใน F

จะได้ว่า $(g(x)) = F[x]$

นั่นคือ $N = F[x]$

ถ้า $q(x)$ มีดีกรี 0

ดังนั้น $q(x) = c$ เมื่อ $c \in F$ และ $c \neq 0$

จะได้ $g(x) = c^{-1}p(x)$

เนื่องจาก $c^{-1}p(x) \in (p(x))$

นั่นคือ $g(x) \in (p(x))$

ดังนั้น $N = (p(x))$

แสดงว่า $(p(x))$ เป็นแม็กซิมัลไอดีลของ $F[x]$

<u>ตัวอย่าง 7.3.2.3</u> จากตัวอย่าง 7.3.2.2 แสดงให้เห็นว่า $x^3 + \bar{3}x + \bar{2}$ เป็นโพลิโนเมี่ยลเฉพาะใน $I_5(x)$ และจากทฤษฎี 7.3.2.2 ได้ว่า $(x^2 + \bar{3}x + \bar{2})$ เป็นแม็กซิมัลไอดีลใน $I_5(x)$

และจากทฤษฎี 5.4.2 ได้ว่า $\dfrac{I_5(x)}{x^2 + \bar{3}x + \bar{2}}$ เป็นฟิลด์

7.3.3 <u>การแยกตัวประกอบใน $F(x)$</u>

<u>นิยาม 7.3.3.1</u> ให้ $f(x), g(x) \neq 0 \in F[x]$ จะกล่าวว่า $g(x)$ หาร $f(x)$ ได้ลงตัว $(g(x) / f(x)$ ถ้ามี $q(x) \in F(x)$ ซึ่ง

$f(x) = g(x)q(x)$

<u>ทฤษฎี 7.3.3.1</u> ให้ $p(x)$ เป็นโพลิโนเมี่ยลคณพาะใน $F(x)$, ถ้า $p(x)/r(x)s(x)$ ได้ลงตัว สำหรับ $r(x), s(x) \in F[x]$ จะได้ว่า $p(x)/ r(x)$ หรือ $p(x) / s(x)$

<u>พิสูจน์</u> สมมุติ $p(x) / r(x)\, s(x)$

นั่นคือ $r(x)\, s(x) = p(x)\, q(x)$ สำหรับบาง $q(x) \in F(x)$

แสดงว่า $r(x)\, s(x) \in (p(x))$

เนื่องจาก $p(x)$ เป็นโพลิโนเมี่ยลเฉพาะ

จากทฤษฎี 7.3.2.2. และ ทฤษฎี 4.4.2 จะได้ว่า $(p(x))$ เป็นไอดีลเฉพาะ

ดังนั้น $r(x) \varepsilon (p(x))$ หรือ $s(x) \varepsilon (p(x))$

นั่นคือ $p(x) / r(x)$ หรือ $p(x) / s(x)$

<u>บทแทรก 7.3.3.2</u> ถ้า $p(x)$ เป็นโพลิโนเมี่ยลเฉพาะใน $F(x)$ และ

$p(x)/r_1(x)r_2(x)\ldots\ldots\ldots\ldots r_n(x)$ สำหรับ $r_i(x) \varepsilon F(x)$ แล้วจะได้ว่า

$p(x) / r_i(x)$ สำหรับบางโพลิโนเมี่ยล $r_i(x) \varepsilon F(x)$ เมื่อ $1 \leq i \leq n$

<u>พิสูจน์</u> แบบฝึกหัด

<u>ทฤษฎี 7.3.3.3</u> ถ้า F เป็นฟิลด์แล้ว จะได้ว่าทุกๆโพลิโนเมี่ยล $f(x)$ ซึ่งไม่ใช่โพลิโนเมี่ยลค่าคงที่ ใน $F(x)$ จะสามารถแยกตัวประกอบใน $F(x)$ ได้เป็นผลคูณของโพลิโนเมี่ยลเฉพาะแบบเดียว และการมีสมาชิกที่เป็นยูนิตเป็นตัวประกอบหนึ่ง

<u>พิสูจน์</u> ให้ $f(x) \varepsilon F(x)$ โดยที่ $f(x)$ ไม่ใช่โพลิโนเมี่ยลค่าคงที่ ถ้า $f(x)$ ไม่เป็นโพลิโนเมี่ยลเฉพาะ

ดังนั้น $f(x) = g(x)\, h(x)$ เมื่อดีกรีของ $g(x)$ และ $h(x)$ เป็นบวกและน้อยกว่าดีกรีของ $f(x)$

ถ้า $g(x)$ และ $h(x)$ เป็นโพลิโนเมี่ยลเฉพาะทั้งคู่ ก็จะได้ว่าทฤษฎีเป็นจริง

ถ้า $g(x)$ และ $h(x)$ ไม่เป็นโพลิโนเมี่ยลเฉพาะ

จะได้ว่า $g(x)$ และ $h(x)$ จะแยกตัวประกอบได้เป็นโพลิโนเมี่ยลที่มีดีกรีลดลงไปอีก กระทำไปเรื่อยๆในที่สุดจะได้

$$f(x) = p_1(x)p_2(x)\ldots\ldots p_r(x) \text{ เมื่อ } p_i(x) \text{ เป็นโพลิโนเมี่ยลเฉพาะ}$$

ต่อไปจะพิสูจน์ว่า $f(x)$ เขียนเป็นผลคูณของโพลิโนเมี่ยลเฉพาะได้เพียงแบบเดียว

สมมุติให้ $f(x) = p_1(x)p_2(x).....p_r(x)$ เมื่อ $p_i(x)$ เป็นโพลิโนเมี่ยลเฉพาะ

$1 \leq i \leq r$

และ $f(x) = q_1(x)q_2(x)..q_s(x)$ เมื่อ $q_j(x)$ เป็นโพลิโนเมี่ยลเฉพาะ

$1 \leq j \leq s$

เนื่องจาก $p_1(x) / f(x)$

นั่นคือ $p_1(x) / q_1(x)q_2(x) .... q_s(x)$

จากบทแทรก 7.3.3.2 จะได้ว่า $p_1(x)/q_j(x)$ สำหรับบาง j เมื่อ $1 \leq j \leq s$

สมมุติให้ $j = 1$

ดังนั้น $p_1(x) / q_1(x)$

เนื่องจาก $q_1(x)$ เป็นโพลิโนเมี่ยลเฉพาะ

ดังนั้น $q_1(x) = u_1p_1(x)$ เมื่อ $u_1 \neq 0$

แต่ $u_1 \varepsilon F$ นั่นคือ u_1 เป็นยูนิต

จะได้ว่า $p_1(x)p_2(x) ....p_r(x) = u_1p_1(x)q_2(x) .... q_s(x)$

โดยอาศัยกฎการตัดออกสำหรับการคูณใน $F[x]$

จะได้ $p_2(x) .... p_r(x) = u_1q_2(x) .... q_s(x)$

ในทำนองเดียวกันจะได้ว่า $q_2(x) = u_2p_2(x)$

ดังนั้น $p_3(x) .... q_r(x) = u_1u_2q_3(x) ...... q_s(x)$

กระทำเช่นนี้ต่อไปเรื่อยๆ ในที่สุดจะได้ว่า

$e = u_1u_2 .... u_rq_{r+1}(x) ..... q_s(x)$ โดยที่ u_i เป็นยูนิต

ดังนั้นจะได้ว่า $r = s$
นั่นคือโพลิโนเมี่ยล $p_i(x)$ และ $q_i(x)$ จะเหมือนกันนอกเสียจากการเรียงลำดับและการมีสมาชิกที่เป็นยูนิตเป็นตัวประกอบ

แบบฝึกหัด 7 ข

1. จงพิสูจน์ว่า ถ้า $f(x)$ และ $g(x)$ เป็นสมาชิกที่ไม่ใช่โพลิโนเมี่ยลศูนย์ใน $R[x]$ เมื่อ $R[x]$ คือโพลิโนเมี่ยลริง และ R เป็นริง แล้วจะได้ว่าดีกรี $[f(x)g(x)]$ = ดีกรี $f(x)$ + ดีกรี $g(x)$
2. ให้ R เป็นริง , $R[x]$ เป็นโพลิโนเมี่ยลริง ถ้า $f(x)$ และ $g(x)$ เป็นสมาชิกที่ไม่ใช่โพลิโนเมี่ยลศูนย์ใน $R[x]$ แล้วจะได้ว่าดีกรี $f(x) \leq$ ดีกรี $f(x)g(x)$
3. ให้ R เป็นริง , $R[x]$ เป็นโพลิโนเมี่ยลริง จงพิสูจน์ว่าถ้า R ไม่มีตัวหารศูนย์แล้ว $R[x]$ ก็จะไม่มีตัวหารศูนย์
4. จงพิสูจน์ว่าโพลิโนเมี่ยลริง $R[x]$ เป็นอินติกรัลโดเมนก็ต่อเมื่อ ริง R เป็นอินติกรัลโดเมน
5. จงพิสูจน์ว่า ถ้า F เป็นฟิลด์ , $F[x]$ เป็นโพลิโนเมี่ยลริง แล้ว $F(x)$ จะเป็นอินติกรัลโดเมน
6. จงแสดงว่า $Q(x)/(x^2 - 2)$ เป็นฟิลด์ เมื่อ Q เป็นฟิลด์ของจำนวนตรรกยะ และ $Q[x]$ เป็นโพลิโนเมี่ยลริง
7. จงพิสูจน์บทแทรก 7.3.6
8. ให้ $f(x) = x^6 + \bar{3}x^5 + \bar{4}x^2 - \bar{3}x + \bar{2}$ และ $g(x) = x^2 + \bar{2}x - \bar{3}$ เป็นสมาชิกใน $I_7(x)$ จงหา $q(x)$ และ $r(x)$ ใน $I_7(x)$ ซึ่งทำให้

$f(x) = g(x)q(x) + r(x)$ เมื่อดีกรี $r(x) < 2$

9. จงแยกตัวประกอบของ $x^4 + 4$ เป็นตัวประกอบใน $I_5[x]$

10. จงแสดงว่า $f(x) + x^2 + 8x - 2$ เป็นโพลิโนเมี่ยลเฉพาะใน $F[x]$ เมื่อ F เป็นฟิลด์ของจำนวนตรรกยะ และ $f(x)$ จะเป็นโพลิโนเมี่ยลเฉพาะหรือไม่ เมื่อ F เป็นฟิลด์ของจำนวนจริง และจำนวนเชิงซ้อน

11. จงแสดงว่า $x^4 - 22x^2 + 1$ เป็นโพลิโนเมี่ยลเฉพาะใน $F[x]$ เมื่อ F เป็นฟิลด์จำนวนตรรกยะ

12. ถ้า F เป็นฟิลด์ และ $a \neq 0$ เป็น zero ของ $f(x) = a_0 + a_1x + \cdots\cdots + a_nx^n$ ใน $F[x]$ จงแสดงว่า $\frac{1}{a}$ เป็น zero ของ $a_n + a_{n-1}x + \cdots\cdots + a_0x^n$

13. ให้ F เป็นฟิลด์ และ $f(x), g(x) \in F[x]$ จงแสดงว่า $f(x)$ หาร $g(x)$ ได้ลงตัว ก็ต่อเมื่อ $g(x) \in (f(x))$

14. ให้ F เป็นฟิลด์ และให้ $f(x), g(x) \in F(x)$ จงแสดงว่า

$$N = \{ r(x)f(x) + s(x)g(x) \mid r(x), s(x) \in F(x)\}$$

เป็นไอดีลของ $F(x)$
