บทที่ 7
การแยกตัวประกอบของพหุนาม
(Factorization of Polynomials)

7.1 การแยกตัวประกอบของพหุนามบนสนาม
(Factorization of Polynomial over a field)

ในหัวข้อนี้ เราจะพิจารณาการแยกตัวประกอบเหนือวงพหุนาม เรามุ่งที่จะหาเงื่อนไขที่จำเป็นและเพียงพอบน R ที่จะทำให้เรามั่นใจได้ว่าเมื่อใดแต่ละสมาชิกของ $R[x]$ สามารถจะแยกตัวประกอบได้

ทฤษฎี 7.1.1 สมาชิก $a \in F$ จะเป็นศูนย์ของ $f(x) \in F[x]$ ก็ต่อเมื่อ $x - a$ เป็นตัวประกอบตัวหนึ่งของ $f(x) \in F[x]$

พิสูจน์

$\Rightarrow$ สมมติ $a \in F$ เป็นศูนย์ของ $f(x) \in F[x]$

$\therefore$ สำหรับ $a \in F$ เราได้ $f(a) = 0$

ให้ $(x - a) \in F[x]$

โดยทฤษฎี 6.1.4 (ขั้นตอนวิธีการหาร)

จะต้องมี $q(x), r(x) \in F[x] \ni$

$$f(x) = (x - a)q(x) + r(x)$$

โดยที่ $\deg(r(x)) < \deg(x - a)$

.$\deg(r(x)) < 1$

.$r(x) = c$ สำหรับบาง $c \in F$

.$f(x) = (x \quad a)\ q(x) + c$

โดยทฤษฎี 6.2.2

ถ้า $\psi_a : \ F[x] \to E$ จะได้

$$\psi_a(f(x)) = \psi_a((x - a)\ q(x) + c)$$

$$f(a) = (a - a)\ q(a) + c$$

$$c$$

แต่ $f(a) = 0'$

$$c = 0$$

. $f(x) = (x - a)\ q(x)$

แสดงว่า $f(x)$ สามารถเขียนได้เป็น $(x - a)q(x)$

ดังนั้น $(x - a)$ เป็นตัวประกอบของ $f(r)$

$\Leftarrow$ สมมติ $(x - a)$ เป็นตัวประกอบหนึ่งของ $f(x)$

.. $f(x) = (x \quad a)\ h(x)$ สำหรับบาง $h(x) \in F[x]$

$$\psi_a(f(x)) = \psi_a((x - a)h(x))$$

$$= (a - a)h(a)$$

$$= 0$$

แต่ $\psi_a(f(x)) = f(a)$

$$f(a) = 0$$

แสดงว่า a เป็นศูนย์ของ $f(x)$ #

ทฤษฎี 7.1.2 พหุนาม $0 \neq f(x) \in F[x]$ ซึ่งมีลำดับขั้น n จะมีศูนย์ของ $f(x)$ ในสนาม F ได้อย่างมาก n ตัว

พิสูจน์

จากทฤษฎี 7.1.1 จะได้ว่า

ถ้า $a_1 \in F$ เป็นศูนย์ของ $f(x)$ แล้ว

$$f(x) = (x - a_1)\, q_1(x)$$

โดยที่ $\deg(q_1(x)) = n - 1$

และถ้า $a_2 \in F$ เป็นศูนย์ของ $q_1(x)$ แล้ว

$$f(x) = (x - a_1)(x - a_2)\, q_2(x)$$

โดยขบวนการนี้ เราจะได้

$$f(x) = (x - a_1)(x - a_2) \ldots (x - a_r)\, q_r(x)$$

โดยที่ $q_r(x)$ ไม่มีศูนย์ใน F อีกต่อไป

และแน่นอน $r \leqslant n$

ถ้า $b \neq a_i$ สำหรับ $i = 1, 2, \ldots, r$ และ $b \in F$ แล้ว

$$f(b) = (b - a_1)(b - a_2) \ldots (b - a_r)\, q_r(b) \neq 0$$

เนื่องจาก F ไม่มีตัวหารของศูนย์

และโดยการสร้างทั้ง $b - a_i$ และ $q_r(b)$ ไม่ใช่ศูนย์

ด้วยเหตุนี้ a_i สำหรับ $i = 1, 2, \ldots, r \leqslant n$ ทั้งหมดเป็นศูนย์ของ $f(x)$ ใน F

ตัวอย่าง 7.1.1 สำหรับพหุนาม $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1 \in Z_5[x]$ ถ้าหาร $f(x)$ ด้วย $g(x) = x^2 - 2x + 3$ เพื่อหา $q(x)$ และ $r(x)$ ของทฤษฎี 6.2.2 เราจะทำโดยการหารยาว

แต่ต้องไม่ลืมว่าเราทำในสนาม $Z_5[x]$

ดังนั้น เช่น $4x - (-3x) = 2x$ ไม่ใช่ $7x$

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

ดังนั้น $x^4 - 3x^3 + 2x^2 + 4x - 1 = [(x^2 - 2x + 3)(x^2 - x - 3)] + (x + 3)$

ดังนั้น $q(x) = x^2 - x - 3$ และ $r(x) = (x + 3)$

ตัวอย่าง 7.1.2 พิจารณาใน $Z_5[x]$ อีกครั้ง

ขอให้สังเกตว่า 1 เป็นศูนย์ของ

$$(x^4 + 3x^3 + 2x + 4) \in Z_5[x]$$

ดังนั้น โดยทฤษฎี 7.1.1 เราสามารถแยกตัวประกอบ

$$x^4 + 3x^3 + 2x + 4 = (x - 1)\, q(x) \in Z_5[x]$$

เพื่อสะดวกเราจะทำโดยการหารยาว

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

$$4x^2 \quad 4x$$

$$x + 4$$

$$x - 1$$

$$0$$

ดังนั้น $x^4 + 3x^3 + 2x + 4 = (x - 1)(x^3 + 4x^2 + 4x + 1)$ ใน $Z_5[x]$
เนื่องจาก 1 เป็นศูนย์ของ $x^3 + 4x^2 + 4x + 1$ ด้วย เราจึงสามารถหารพหุนามนี้ ด้วย $x - 1$ และได้

$$\begin{array}{r|l} & x^2 + 4 \\ \hline x - 1 & x^3 + 4x^2 + 4x + 1 \\ & \underline{x^3 - x^2} \\ & \quad 0 + 4x + 1 \\ & \qquad 4x - 4 \\ & \qquad\quad 0 \end{array}$$

และเนื่องจาก 1 ยังคงเป็นศูนย์ของ $x^2 + 4$ อีกด้วย เราจึงหารด้วย $x - 1$ อีกครั้ง และได้

$$\begin{array}{r|l} & x + 1 \\ \hline x^2 - 1 & x^2 \qquad + 4 \\ & \underline{x^2 - x} \\ & \quad x + 4 \\ & \quad \underline{x - 1} \\ & \qquad 0 \end{array}$$

ดังนั้น $x^4 + 3x^3 + 2x + 4 = (x - 1)^3(x + 1) \in Z_5[x]$ #

7.2 พหุนามลดทอนไม่ได้
(Irreducible polynomials)

ในหัวข้อนี้เราจะมาพิจารณาพหุนามที่ลดทอนไม่ได้ (Irreducible polynomials)

นิยาม ให้ $f(x)$ เป็นพหุนามที่ไม่ใช่พหุนามค่าคงตัว และ $f(x) \in F[x]$ $f(x)$ จะเป็นพหุนามลดทอนไม่ได้ ใน $F[x]$ เมื่อ $f(x)$ ไม่สามารถเขียนได้ในรูปผลคูณ $g(x)\,h(x)$ โดยที่ $g(x)$ และ $h(x)$ เป็นพหุนามใน $F[x]$ และลำดับขั้นของทั้ง $g(x)$ และ $h(x)$ น้อยกว่าลำดับขั้นของ $f(x)$

ตัวอย่าง 7.2.1 $x^2 - 2 \in Q[x]$ ไม่มีศูนย์ใน Q
แสดงว่า $x^2 - 2$ ไม่สามารถลดทอนได้เหนือ Q
แต่อย่างไรก็ตาม $x^2 - 2 \in R[x]$ สามารถแยกตัวประกอบได้เหนือ R
เพราะ $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

ตัวอย่าง 7.2.2 $f(x) = x^3 + 3x + 2 \in Z_5[x]$ เป็นพหุนามลดทอนไม่ได้ใน Z_5 เพราะถ้าสมมติ $f(x)$ แยกตัวประกอบได้ใน $Z_5[x]$ แล้วอย่างน้อยที่สุดต้องมีตัวประกอบตัวหนึ่งของ $f(x)$ อยู่ในรูป $(x - a)$ สำหรับบาง $a \in Z_5$ แล้วโดยทฤษฎี 7.1.1 จะได้ต่อไปว่า $f(a) = 0$
แต่อย่างไรก็ตามเราพบว่า

$f(0) = 2$

$f(1) = 1$

$f(2) = 1$

$f(3) = 3$

$f(4) = 3$

ดังนั้นจะเห็นว่า $f(x)$ ไม่มีศูนย์ใน Z_5

แสดงว่า $f(x)$ แยกตัวประกอบไม่ได้

$\therefore$ $f(x)$ เป็นพหุนามลดทอนไม่ได้ เหนือ Z_5 #

ทฤษฎี 7.2.1 ให้ $f(x) \in F[x]$ และให้ $f(x)$ มีลำดับขั้น 2 หรือ 3 แล้ว $f(x)$ ลดทอนได้เหนือ F ก็ต่อเมื่อ $f(x)$ มีศูนย์ใน F

พิสูจน์

$\Rightarrow$ ให้ $f(x)$ ลดทอนได้เหนือ F ($f(x)$ แยกตัวประกอบได้)

$\therefore$ $f(x) = g(x)\,h(x)$

โดยที่ deg $(g(x))$ และ deg $(h(x))$ น้อยกว่า deg $(f(x))$

แต่ deg $(f(x)) = 2$ หรือ 3

$\therefore$ deg $(g(x))$ หรือ มิฉะนั้นก็ $g(h(x)) = 1$

สมมติ deg $(g(x)) = 1$

เพื่อให้ได้ $f(x) \in F[x]$ $g(x)$ ต้องอยู่ในรูป $(x - a)$

$$\therefore \quad g(a) = (a - a)$$
$$= 0$$

$$\therefore \quad f(a) = (x - a)\,h(x)$$
$$= 0$$

$\therefore$ $f(x)$ มีศูนย์ใน F

$\Leftarrow$ สมมติ f(x) มีศูนย์ใน F

โดยทฤษฎี 7.1.1 ได้ว่า

ถ้า $f(a) = 0$ สำหรับ $a \in F$ แล้ว $(x - a)$ ต้องเป็นตัวประกอบหนึ่งของ f(x)

$\therefore f(x) = (x - a)\, r(x)$

$\therefore$ f(x) ลดทอนได้ #

นิยาม ถ้า R เป็นวงที่มี unity และสอดคล้องกฎการสลับที่ และ $a \in R$ กลุ่มอุดมคติ $\{ra \mid r \in R\}$ เป็นกลุ่มอุดมคติหลัก ก่อกำเนิดโดย a เขียนแทนด้วย $<a>$ และกลุ่มอุดมคติ I ของ R เป็นกลุ่มอุดมคติหลัก ถ้า $I = <a>$ สำหรับบาง $a \in R$

ทฤษฎี 7.2.2 ถ้า F เป็นสนามแล้วทุก ๆ กลุ่มอุดมคติ $I \in F[x]$ เป็นกลุ่มอุดมคติหลัก

พิสูจน์

ให้ I เป็นกลุ่มอุดมคติของ F[x]

ถ้า $I = \{0\}$ แล้ว $I = <0>$

ถ้า $I \neq \{0\}$

ให้ g(x) เป็นสมาชิกที่ไม่ใช่ศูนย์ และมีลำดับขั้นน้อยที่สุดของ I

ถ้า $\deg(g(x)) = 0$ แล้ว $g(x) \in F$ และเป็น unit

ดังนั้น $I = F[x] = <1>$

$\therefore$ I เป็นกลุ่มอุดมคติหลัก

ถ้า $\deg(g(x)) \geq 1$

ให้ $f(x) \in I$

$\therefore f(x) = g(x)q(x) + r(x)$

โดยที่ $\deg(r(x)) < \deg(g(x))$

$\because f(x) \in I, g(x) \in I$

$\therefore r(x) = f(x) - g(x)q(x) \in I$

เนื่องจาก $g(x)$ เป็นสมาชิกที่ไม่ใช่ศูนย์ และมีลำดับขั้นน้อยที่สุดของ I

$\therefore r(x) = 0$

ดังนั้น $f(x) = g(x)q(x)$

$\therefore I = \langle g(x) \rangle$ #

ทฤษฎี 7.2.3 กลุ่มอุดมคติ $\langle p(x) \rangle \neq 0$ ของ $F[x]$ จะเป็นกลุ่มอุดมคติใหญ่สุดก็ต่อเมื่อ $p(x)$ เป็นพหุนามที่ลดทอนไม่ได้ เหนือ F

พิสูจน์

$\Rightarrow$ สมมติ $\langle p(x) \rangle \neq 0$ เป็นกลุ่มอุดมคติใหญ่สุดของ $F[x]$

$\therefore \langle p(x) \rangle \neq F[x]$

$\therefore p(x) \notin F$

ให้ $p(x) = f(x)g(x)$ สำหรับบาง $f(x), g(x) \in F[x]$

เนื่องจาก $\langle p(x) \rangle$ เป็นกลุ่มอุดมคติใหญ่สุดของ $F[x]$

และด้วยเหตุนี้เป็นกลุ่มอุดมคติจำนวนเฉพาะด้วย

$\because (f(x)g(x)) \in \langle p(x) \rangle$

$\therefore$ $f(x) \in <p(x)>$ หรือ $g(x) \in <p(x)>$

นั่นคือ $f(x)$ หรือมิฉะนั้นก็ $g(x)$ มี $p(x)$ เป็นตัวประกอบ

แต่เราไม่สามารถจะมีทั้งลำดับขั้นของ $f(x)$ และลำดับขั้นของ $g(x)$ ที่น้อยกว่าลำดับขั้นของ $p(x)$ ได้

แสดงว่า $p(x)$ เป็นพหุนามที่ลดทอนไม่ได้ เหนือ F

$\Leftarrow$ สมมติ $p(x)$ เป็นพหุนามที่ลดทอนไม่ได้เหนือ F

และสมมติ N เป็นกลุ่มอุดมคติ $\ni$ $<p(x)> \subsetneq N \subsetneq F[x]$

โดยทฤษฎี 7.2.2 N เป็นกลุ่มอุดมคติหลัก

$\therefore N = <g(x)>$ สำหรับ บาง $g(x) \in N$

และ $p(x) \in N$

$\therefore p(x) = g(x)\, q(x)$ สำหรับ บาง $q(x) \in F[x]$

แต่ $p(x)$ เป็นพหุนามที่ลดทอนไม่ได้

$\therefore$ $\deg(g(x)) = 0$ หรือมิฉะนั้นก็ $\deg(q(x)) = 0$

ถ้า $\deg(g(x)) = 0$ แล้ว $g(x)$ เป็นพหุนามค่าคงตัวใน F

$\therefore g(x)$ เป็น unit ใน $F[x]$

$\therefore <g(x)> = N = F[x]$

ถ้า $\deg(q(x)) = 0$ แล้ว

$q(x) = c$ โดยที่ $c \in F$

และ $g(x) = \left(\frac{1}{c}\right)(p(x)) \in <p(x)>$

$\therefore N = <p(x)>$

$\therefore <p(x)> \subsetneq N \subsetneq F[x]$ เป็นไปไม่ได้

ดังนั้น $<p(x)>$ เป็นกลุ่มอุดมคติใหญ่สุด #

ทฤษฎี 7.2.4 ให้ $p(x)$ เป็นพหุนามลดทอนไม่ได้ ใน $F[x]$ ถ้า $p(x)$ หาร $r(x)\,s(x)$ ลงตัว สำหรับ $r(x), s(x) \in F[x]$ แล้ว $p(x)$ หาร $r(x)$ ลงตัว หรือมิฉะนั้นก็ $p(x)$ หาร $s(x)$ ลงตัว

พิสูจน์

สมมติ $p(x)$ หาร $r(x)\,s(x)$ ลงตัว

$\therefore$ $r(x)\,s(x) \in \langle p(x) \rangle$ ซึ่งเป็นกลุ่มอุดมคติใหญ่สุดของ $F[x]$ ตามทฤษฎี 7.2.3

ดังนั้น $\langle p(x) \rangle$ เป็นกลุ่มอุดมคติจำนวนเฉพาะ

$\therefore$ $r(x) \in \langle p(x) \rangle$ หรือมิฉะนั้นก็ $s(x) \in \langle p(x) \rangle$

ดังนั้น $p(x)$ หาร $r(x)$ ลงตัว หรือมิฉะนั้นก็ $p(x)$ หาร $s(x)$ ลงตัว #

บทแทรก ถ้า $p(x)$ เป็นพหุนามลดทอนไม่ได้ใน $F[x]$ และ $p(x)$ หารผลคูณ $r_1(x) \ldots r_n(x)$ สำหรับ $r_i[x] \in F[x]$ แล้ว $p(x)$ หาร $r_i(x)$ ลงตัวอย่างน้อยที่สุดหนึ่ง i

ทฤษฎี 7.2.5 ถ้า F เป็นสนามแล้วทุก ๆ พหุนามที่ไม่ใช่พหุนามค่าคงตัว $f(x) \in F[x]$ สามารถจะแยกตัวประกอบ ใน $F[x]$ ออกเป็นผลคูณของพหุนามลดทอนไม่ได้ พหุนามลดทอนไม่ได้นี้ unique นอกจากเป็น 0 หรือ unit ใน F

พิสูจน์

ให้ $f(x) \in F[x]$ เป็นพหุนามที่ไม่ใช่พหุนามค่าคงตัว

ถ้า $f(x)$ เป็นพหุนามลดทอนได้ แล้ว

$f(x) = g(x)\ h(x)$ โดยที่ $\deg(g(x))$ และ $\deg(h(x))$ น้อยกว่า $\deg(f(x))$

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

เราหยุดข้อพิสูจน์ตรงนี้

แต่ถ้า $g(x)$ และ $h(x)$ เป็นพหุนามที่ลดทอนได้

อย่างน้อยที่สุดหนึ่งพหุนามใน 2 พหุนามนี้ จะต้องสามารถแยกตัวประกอบลงมาเป็นผลคูณของพหุนามที่มีลำดับขั้นน้อยกว่า และทำเช่นนี้เรื่อยไป เราจะได้

$$f(x) = p_1(x)\,p_2(x)\dots p_r(x)$$

โดยที่ $p_i(x)$ เป็นพหุนามลดทอนไม่ได้

จึงเหลือแต่เพียงจะต้องแสดงว่า พหุนามนี้ unique

สมมติว่า

$$f(x) = p_1(x)\,p_2(x)\dots p_r(x) = q_1(x)\,q_2(x)\dots q_s(x)$$

เป็นตัวประกอบ 2 ชุดของ $f(x)$ ที่ $p_i(x)$ และ $q_i(x)$ เป็นพหุนามลดทอนไม่ได้

โดยบทแทรกของทฤษฎี 7.2.4

$p_1(x)$ หาร บาง $q_i(x)$ ลงตัว สมมติว่า หาร $q_1(x)$ ลงตัว

เนื่องจาก $q_1(x)$ เป็นพหุนามลดทอนไม่ได้

$q_1(x) = u_1p_1(x)$ โดยที่ $u_1 \neq 0$ แต่ $u_1 \in F$

$\therefore$ u_1 เป็น unit

โดยการแทนค่า $u_1p_1(x)$ ลงใน $q_1(x)$ และตัดออกจะได้

$$p_2(x)\dots p_r(x) = u_1q_2(x)\dots q_s(x)$$

ในทำนองเดียวกัน จะได้ $q_2(x) = u_2p_2(x)$ ดังนั้น

$$p_3(x)\dots p_r(x) = u_1u_2q_3(x)\dots q_s(x)$$

โดยขบวนการนี้ จะได้

$$1 = u_1u_2\dots u_rq_{r+1}(x)\dots q_s(x)$$

ซึ่งจะเป็นไปได้ ถ้า $s = r$

ดังนั้น สมการนี้คือ $1 = u_1u_2 \ldots u_r$

ดังนั้น $p_i(x)$ และ $q_i(x)$ เป็นพหุนามเดียวกัน นอกจากจะเป็น 0 หรือ unit #

7.3 วงยูคลิเดียน

(Euclidean rings)

ในหัวข้อนี้เราจะมาพิสูจน์กันว่า $F[x]$ ที่ F เป็นสนามสอดคล้องลำดับขั้นตอนวิธีการหาร (Division algorithm) ซึ่งสิ่งนี้จะนำไปสู่การกำหนดวงยูคลิเดียน

นิยาม

> วง R ที่สอดคล้องกฎการสลับที่ ซึ่งมีสมาชิกมากกว่า 1 ตัว จะเรียกว่า วงยูคลิเดียน (Euclidean ring) ถ้ามีฟังก์ชัน ρ จาก $R/\{0\}$ ไปในจำนวนเต็มที่ไม่ใช่จำนวนลบ ซึ่งสอดคล้องคุณสมบัติ
>
> 1. ถ้า $a, b \in R$ และ $ab \neq 0$ แล้ว $\rho(ab) \geqslant \rho(a)$
> 2. ถ้า $a, b \in R$ และ $b \neq 0$ แล้ว จะมี $r, s \in R \ni a = bs + r$ โดยที่ $r = 0$ หรือมิฉะนั้นก็ $\rho(r) < \rho(b)$

ตัวอย่าง 7.3.1 วง Z (จำนวนเต็ม) เป็นวงยูคลิเดียน โดยที่ $\rho(n) = |n|$ สำหรับ $n \neq 0$

ตัวอย่าง 7.3.2 ให้ F เป็นสนามกำหนด ρ บน $F/\{0\}$ โดย $\rho(x) = 0$ สำหรับทุก ๆ $0 \neq x \in F$ แล้ว F เป็นวงยูคลิเดียน เพราะ $\rho(xy) \geqslant \rho(x)$ ทุก ๆ $xy \neq 0$

และสำหรับ $x,y \in F$ ซึ่ง $y \neq 0$ เรามี $x = y(y^{-1}x) + 0$
แสดงว่า ลำดับขั้นตอนวิธีการหารเป็นจริง

ตัวอย่าง 7.3.3 ถ้า F เป็นสนามแล้ว $F[x]$ เป็นวงยูคลิเดียน โดยที่สำหรับ $p(x) \in F[x]$ ที่ $p(x) \neq 0$ เรากำหนด $\rho(p(x)) = \deg(p(x))$

ทฤษฎี 7.3.1 ให้ $Z[i] = \{a + b_i | a, b \in Z$ และ $i = \sqrt{-1}\}$ (Gaussian integers) แล้ว $Z[i]$ เป็นวงยูคลิเดียน ถ้า ρ กำหนดโดย $\rho(a + b_i) = a^2 + b^2$ สำหรับ $a + b_i \neq 0$

พิสูจน์

ก่อนอื่นขอให้สังเกตว่า

$$
\begin{aligned}
\rho[(a + b_i)(c + d_i)] &= \rho[(ac \quad bd) + (ad + bc)i] \\
&= (ac - bd)^2 + (ad + bc)^2 \\
&= a^2c^2 + b^2d^2 - 2acbd + a^2d^2 + b^2c^2 + 2abcd \\
&= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\
&= (a^2 + b^2)(c^2 + d') \\
&= \rho(a + b_i)\ \rho(c + d_i)
\end{aligned}
$$

ดังนั้น $\rho[(a + b_i)(c + d_i)] \geqslant \rho(a + b_i)$ เมื่อ $(a + b_i)(c + d_i) \neq 0$
เราจะต้องแสดงว่า $Z[i]$ สอดคล้องลำดับขั้นตอนวิธีการหาร
สมมติ $a + b_i, c + d_i \in Z[i]$ โดยที่ $(c + d_i) \neq 0$

กรณีที่ 1 สมมติ $c + d_i = c + o_i = c$

$\exists$ จำนวนเต็ม $q_1, q_2, r_1, r_2 \ni$

$a = q_1c + r_1$ โดยที่ $0 \leqslant |r_1| < \frac{c}{2}$

และ $b = q_2c + r_2$ โดยที่ $0 \leqslant |r_2| \leqslant \frac{c}{2}$

ดังนั้น $a + b_i = (q_1c + r_1) + (q_2c + r_2)i$

$= (q_1 + q_2i)c + (r_1 + r_2i)$

โดยที่ $r_1 + r_2i = 0$ หรือมิฉะนั้นก็ $\rho(r_1 + r_2i) = r_1^2 + r_2^2$

$$\leqslant \frac{c^2}{4} + \frac{c^2}{4}$$

$$< c^2$$

$$= \rho(c + o_i)$$

กรณีที่ 2 ถ้า $c + d_i$ ไม่ใช่จำนวนเต็ม แล้ว

พิจารณา $(c + d_i)(c - d_i)$ และ $(a + b_i)(c - d_i)$

โดยกรณีที่ 1

$\exists$ Guassian integer $x + y_i$ และ $r + s_i \ni$

$(a + b_i)(c - d_i) = (c + d_i)(c - d_i)(x + y_i) + (r + s_i)$

โดยที่ $r + s_i = 0$ หรือมิฉะนั้นก็ $\rho(r + s_i) < \rho|(c + d_i)(c - d_i)|$

$(c - d_i)|(a + b_i) - (c + d_i)(x + y_i)| = r + s_i$

ถ้า $r + s_i = 0$ แล้ว

เนื่องจาก $Z[i]$ เป็นโดเมนเชิงจำนวนเต็ม และ $c - d_i \neq 0$

$\therefore (a - b_i) - (c + d_i)(x + y_i) = 0$

ด้วยเหตุนี้ $a + b_i = (c + d_i)(x + y_i) + 0$

ถ้า $(r + s_i) \neq 0$ แล้ว $(a + b_i) - (c + d_i)(x + y_i)$ จะต้องเป็น Guassian integer

บางตัวสมมติเป็น $t + u_i$

เนื่องจาก $(c - d_i)(t + u_i) = (r + s_i)$

เราทราบว่า $\rho(c - d_i)\,\rho(t + u_i) = \rho[(c - d_i)(t + u_i)]$

$$= \rho(r + s_i)$$

$$< \rho[(c + d_i)(c - d_i)]$$

$$= \rho(c \quad d_i)\ \rho(c + d_i)$$

ดังนั้น $\rho(t + u_i) < \rho(c + d_i)$

$a + b_i = (c + d_i)(x + y_i) + (t + u_i)$

โดยที่ $\rho(t + u_i) < \rho(c + d_i)$ #

ทฤษฎี 7.3.2 ถ้า R เป็นวงยูคลิเดียน แล้วทุก ๆ กลุ่มอุดมคติของ R เป็นกลุ่มอุดมคติหลัก และถ้า $I = \langle x \rangle$ เป็นกลุ่มอุดมคติของ R แล้ว $I = \{rx | r \in R\}$

พิสูจน์

ให้ I เป็นกลุ่มอุดมคติของ R

ถ้า $I = \{0\}$ แล้ว I เป็นกลุ่มอุดมคติหลักโดยมี 0 เป็นตัวก่อกำเนิด

ถ้า $I \neq \{0\}$ แล้ว

$\rho(y)$ จะเป็นจำนวนเต็มที่ไม่ใช่ 0 สำหรับ $0 \neq y \in I$

ดังนั้น เราสามารถเลือก $x \in I \ni x \neq 0$ และ $\rho(x) \leqslant \rho(y)$ สำหรับทุก ๆ $0 \neq y \in I$

ให้ $y \in I$ แล้ว

โดยลำดับขั้นตอนวิธีการหาร (Division algorithm)

$\exists q, r \in R \ni y = qx + r$ โดยที่ $r = 0$ หรือมิฉะนั้นก็ $\rho(r) < \rho(x)$

แต่ $y \in I$ และ $qx \in I$

เนื่องจาก $x \in I$ และ I เป็นกลุ่มอุดมคติ

ดังนั้น $r = y - qx \in I$

ถ้า $r \neq 0$ แล้วมี $r \in I \ni \rho(r) < \rho(x)$

ซึ่งขัดแย้งกับการเลือก x

ดังนั้น $r = 0$

$\therefore\ y = q(x) \in \langle x \rangle$

$\therefore\ I = \langle x \rangle$

บทแทรก ถ้า $0 \neq I$ เป็นกลุ่มอุดมคติของวงยูคลิเดียนแล้ว $I = \langle b \rangle$ สำหรับ $0 \neq b \in I \ni \rho(b) \leqslant \rho(y);\ 0 \neq y \in I$

ทฤษฎี 7.3.3 ถ้า R เป็นวงยูคลิเดียน แล้ว R มี unity

พิสูจน์

$\because$ R เป็นกลุ่มอุดมคติของ R เอง

$\exists x \in R \ni R = \{xr \mid r \in R\}$

ดังนั้น $\exists y \in R$ โดยที่ $xy = x$

ให้ $r \in I$

$\exists s \in R \ni sx = r$

$\therefore\ r = sx$

$= s(xy)$

$= (sx)y$

$= ry$

$\therefore$ y เป็น ตัวผกผันสำหรับการคูณ

$\therefore$ y เป็น unity ของ R #

นิยาม ถ้า R เป็นวงยูคลิเดียน และเป็นโดเมนเชิงจำนวนเต็ม แล้วเรียก R ว่าโดเมนยูคลิเดียน

ถ้าเราพิจารณาสนามของจำนวนเศษส่วน เราจะสามารถเขียน 2 ได้หลาย ๆ แบบ

เช่น $2 = 2$

หรือ $2 = \left(\frac{1}{2}\right)4$

หรือ $2 = \left(\frac{1}{3}\right)6$

หรือ $2 = \left(\frac{2}{7}\right)\left(\frac{1}{2}\right)(14)$

ฯลฯ

เป็นที่เห็นแจ่มชัดว่า บางแบบจะเขียน 2 ในรูปของผลคูณของตัวประกอบ อย่างไรก็ตาม ถ้าเราสังเกตว่า ในสนามของจำนวนเศษส่วน ทุก ๆ สมาชิกที่ไม่ใช่ศูนย์ จะมีตัวผกผันสำหรับการคูณ และนี่คือคุณสมบัติที่แยก ± 1 ในจำนวนเต็ม

นิยาม ถ้า R เป็นวงที่มี unity และสอดคล้องกฎการสลับที่แล้ว จะเรียก $r \in R$ ว่า unit ถ้ามี $x \in R$ ซึ่ง $xr = 1$ จะกล่าวว่า สมาชิก $r, s \in R$ เป็น associates ถ้ามี unit $x \in R$ ซึ่ง $r = xs$ จะเรียกสมาชิก $p \in R$ ว่า จำนวนเฉพาะ ถ้า p ไม่เป็นทั้ง 0 และ unit และเมื่อไรก็ตาม $p = rs\ (r, s \in R)$ แล้ว r หรือมิฉะนั้นก็ s ต้องเป็น unit

ขอให้นักศึกษาสังเกตว่า นิยามนี้กำหนดขึ้นมาสำหรับวงที่มี unity และสอดคล้องกฎการสลับที่เท่านั้น ไม่ได้กำหนดสำหรับ วงยูคลิเดียน

ตัวอย่าง 7.3.4 ถ้า F เป็นสนามแล้วสมาชิกทุกตัวที่ไม่ใช่ 0 ของ F เป็น unit และสำหรับสมาชิก 2 ตัวใด ๆ ที่ไม่ใช่ 0 ของ F เป็น associate เนื่องจากสมาชิกทุกตัวของ F จะต้องเป็น 0 หรือมิฉะนั้นก็เป็น unit จึงไม่มีจำนวนเฉพาะ

ตัวอย่าง 7.3.5 ใน Z สมาชิกที่เป็น unit คือ 1 และ -1 ถ้า n เป็นจำนวนเต็มที่ไม่ใช่ 0 แล้ว n และ $-n$ เท่านั้น ที่เป็น associate ของ n

ตัวอย่าง 7.3.6 ใน $Z[i]$ สมาชิกที่เป็น unit มีเฉพาะ $1, -1, i, -i$ เพราะว่า ถ้า $a + b_i$ เป็น unit แล้ว จะมีสมาชิก $c + d_i$ ของ $Z[i]$ ซึ่ง $(a + b_i)(c + d_i) = 1$ อย่างไรก็ตาม จากทฤษฎี 7.3.1 เราได้ทำแล้วว่า

$$\rho[(a + b_i)(c + d_i)] = \rho(a + b_i)\,\rho(c + d_i)$$

ดังนั้น $\rho(a + b_i) = a^2 + b^2$

$= 1$

$= (c + d_i)$

$= c^2 + d^2$

และด้วยเหตุนี้ 1, − 1, i, -i เท่านั้นที่เป็น unit

และ associates ของ a + b, คือ l(a + b_i), − 1(a + b_i), i(a + b_i) และ − i(a + b_i)

ทฤษฎี 7.3.4 ถ้า R เป็นโดเมนยูคลิเดียน และ $x, y \in R$ เป็นสมาชิกที่ไม่ใช่ศูนย์ และเป็น associate แล้ว $\rho(x) = \rho(y)$

พิสูจน์

เนื่องจาก x, y เป็น associate

$\exists$ unit $u, v \in R \ni x = uy$ และ $y = vx$

$\rho(x) = \rho(uv) \geqslant \rho(y)$

และ $\rho(y) = \rho(vx) \geqslant \rho(x)$

$\therefore \rho(x) = \rho(y)$ #

นิยาม ถ้า R เป็นวงที่สอดคล้องกฎการสลับที่ และ $x, y \in R$ โดยที่ $x \neq 0$ แล้ว จะกล่าวว่า x หาร y ลงตัว เขียนแทนด้วย $x|y$ เมื่อมี $z \in R \ni xz = y$

ข้อสังเกต ถ้า R เป็นวงที่มี unity และสอดคล้องกฎการสลับที่แล้ว ข้อความต่อไปนี้เป็นจริง

1. ถ้า u เป็น unit และ $x \in R$ แล้ว $u|x$
2. ถ้า $x, y, z \in R \ni x|y$ และ $x|z$ แล้ว $x|(az + by)$ สำหรับ $a, b \in R$

นักศึกษาคงยังจำเรื่องตัวหารร่วมมากของจำนวนเต็มสองจำนวน m, n (ทั้ง m และ n ไม่ใช่ 0) จำนวนเต็มบวก d จะเรียกว่า ตัวหารร่วมมากของ m และ n ถ้า $d|m$ และ $d|n$ และเมื่อใดก็ตาม $k|m$ และ $k|n$ แล้ว $k|d$ เราจะขยายแนวความคิดนี้ออกไปยังวงที่มี unity และสอดคล้องกฎการสลับที่

นิยาม ให้ R เป็นวงที่มี unity และสอดคล้องกฎการสลับที่ $r, s \in R$ (ทั้ง r และ s ไม่ใช่ศูนย์ทั้งคู่) จะเรียกสมาชิก $d \in R$ ว่าตัวหารร่วมมากของ r และ s ถ้า $d|r$ และ $d|s$ และเมื่อใดก็ตามที่มี $t \in R \ni t|r$ และ $t|s$ แล้ว $t|d$ ใช้สัญลักษณ์ $d = (r, s)$ จะเรียกสมาชิก $r, s \in R$ ว่า จำนวนเฉพาะสัมพัทธ์ (relatively prime) ถ้าตัวหารร่วมมากของ r และ s คือ 1 ใช้สัญลักษณ์ $1 = (r, s)$

ข้อสังเกต ถ้า R เป็นโดเมนเชิงจำนวนเต็มที่มี unity และ $x, y \in R \ni x|y$ และ $y|x$ แล้ว x และ y เป็น associate

ทฤษฎี 7.3.5 ถ้า R เป็นโดเมนยูคลิเดียน $x, y \in R$ (ทั้ง x และ y ไม่ใช่ศูนย์) แล้วจะมีตัวหารร่วมมากของ x และ y ใน R และถ้า d เป็นตัวหารร่วมมาก ของ x และ y แล้วจะมี $a, b \in R \ni d = ax + by$

พิสูจน์

พิจารณา $I = \{rx + sy | r, s \in R\}$

ขอให้สังเกตว่า I เป็นกลุ่มอุดมคติ และเป็นกลุ่มอุดมคติหลักโดย

$I = \langle ax + by \rangle$

$\because$ $x = 1x + 0y \in I$

และ $y = 0x + 1y \in I$

เราทราบว่า $d|x$ และ $d|y$

$\therefore d = (ax + by)$

ถ้า $z \in R \ni z|x$ และ $z|y$ แล้ว $z|d$

$\therefore$ d เป็นตัวหารร่วมมากของ x และ y

และเราสามารถเขียน $d = (ax + by)$ #

ทฤษฎี 7.3.6

ให้ R เป็นโดเมนยูคลิเดียน $x, y, z \in R \ni (x, y) = 1$ ถ้า $x|yz$ แล้ว $x|z$

พิสูจน์

$\because (x, y) = 1$

โดยทฤษฎี 7.3.5 ได้ว่า

มี $a, b \in R \ni ax + by = 1$

$axz + byz = z$

และ $x|axz$ และ $x|byz$ ($\because x|yz$)

$x|(axz + byz)$

$\therefore x/z$ #

บทแทรก ถ้า R เป็นโดเมนยูคลิเดียน และ p เป็นจำนวนเฉพาะของ R $\ni p|xy$ โดยที่ $x, y \in R$ แล้ว $p|x$ หรือมิฉะนั้นก็ $p|y$

ทฤษฎี 7.3.7 ถ้า R เป็นโดเมนยูคลิเดียน และ $x \in R \ni \rho(x) \leqslant \rho(r)$ สำหรับทุก ๆ $r \in R/\{0\}$ แล้ว x เป็น unit

พิสูจน์

ถ้า $0 \neq r \in R$ แล้ว

$$\rho(r) = \rho(r1) \geqslant \rho(1)$$

ดังนั้น $\rho(x) \geqslant \rho(1)$

แต่ $\rho(x) \leqslant \rho(r)$ (โจทย์)

$\because$ $\rho(x) \leqslant \rho(1)$

$\therefore$ $\rho(x) = \rho(1)$

โดยบทแทรกของทฤษฎี 7.3.2

$\therefore$ x เป็น associate ของ 1

$\therefore$ x เป็น unit #

ทฤษฎี 7.3.8 ให้ R เป็นโดเมนยูคลิเดียน $0 \neq x \in R$ โดยที่ x ไม่ใช่ unit แล้ว $\rho(xy) > \rho(y)$ สำหรับทุก ๆ $0 \neq y \in R$

พิสูจน์

$\because \rho(xy) \geqslant \rho(y)$

ถ้า $\rho(xy) = \mathbf{p(y)}$ แล้ว

$\langle y \rangle = \langle xy \rangle$

ดังนั้น จะมี $r \in R \ni rxy = y$

$\therefore (rx - 1)y = 0$

แต่ R เป็นโดเมนเชิงจำนวนเต็ม และ $y \neq 0$

ดังนั้น $rx - 1 = 0$

และ $rx = 1$

ดังนั้น x เป็น unit

ซึ่งขัดแย้งกับข้อกำหนดของทฤษฎี (x ไม่ใช่ unit)

$\therefore \rho(xy) > \rho(y)$ #

มาถึงตรงนี้เรามีความรู้พร้อมที่จะพิสูจน์ Unique factorization Theorem แล้ว แต่ก่อนอื่นขอให้มาพิจารณาความหมายของคำว่า unique ในที่นี้กันก่อนว่า เราหมายความว่าอย่างไร

ให้ $x = up_1p_2$ โดยที่ p_1 และ p_2 เป็นจำนวนเฉพาะ

และ u เป็น unit

ถ้า $vw = 1$ แล้ว up_1 และ vp_1 เป็นจำนวนเฉพาะด้วย

และ $x = (uww)(vp_1)(vp_2)$

ดังนั้น เราได้แยก (ตัวประกอบ) x ออกเป็นหนึ่งเท่าผลคูณ (unit times product) ของกำลังจำนวนเฉพาะใน 2 ทาง

สำหรับการแยกตัวประกอบให้เป็น unique เราหมายถึง จำนวนเฉพาะจำนวนเดียวกัน หรือ associate ของจำนวนเฉพาะจำนวนเดียวกัน จะต้องปรากฏเป็นกำลังเดียวกัน นั่นคือ

ให้ $x = u_1 p_1^{\alpha_1} \cdots p_n^{\alpha_n} = v q_1^{\beta_1} \cdots q_k^{\beta_k}$

โดยที่ u และ v เป็น unit

p_i's และ q_i's เป็นจำนวนเฉพาะ

p_i ไม่เป็น associate ของ p_j สำหรับ $i \neq j$

q_i ไม่เป็น associate ของ q_j สำหรับ $i \neq j$

โดย unique เราหมายความว่า

$k = n$ และแต่ละ p_i เป็น associate ของบาง q_j และ $\alpha_i = \beta_j$

ทฤษฎี 7.3.9 (Unique factorization Theorem)
ในโดเมนยูคลิเดียน สมาชิกทุกตัวที่ไม่ใช่ 0 หรือ unit สามารถจะเขียนได้เป็นหนึ่งเท่าของผลคูณของกำลังของจำนวนเฉพาะ

พิสูจน์

ก่อนอื่นเราจะพิสูจน์ก่อนว่า แต่ละสมาชิกสามารถจะแยก (ตัวประกอบ) ได้อย่างในทฤษฎี ข้อพิสูจน์จะต้องใช้การอุปมานบน $\rho(x)$; $x \in R$

ให้ $x \in R$ โดยที่ $\rho(x) \leqslant \rho(r)$ สำหรับทุก ๆ $r \in R$

โดยทฤษฎี 7.3.6 x เป็น unit

ทฤษฎีสอดคล้อง

สมมติ สำหรับ $r \in R$ ซึ่ง $\rho(1) \leqslant \rho(r) < k$ สามารถจะแยก (ตัวประกอบ) ได้เป็นหนึ่งเท่าของผลคูณของกำลังของจำนวนเฉพาะ

ให้ $s \in R$ โดยที่ $\rho(s) = k$

ถ้า s เป็นจำนวนเฉพาะ แล้ว

$s = 1s$ สอดคล้องทฤษฎี

ถ้า s ไม่ใช่จำนวนเฉพาะแล้ว

$s = tr$ สำหรับ บาง t และ $r \in R$ โดยที่ทั้ง r และ t ไม่ใช่ unit

โดทฤษฎี 7.3.7

$\rho(s) = \rho(tr) > \rho(r)$

และ $\rho(s) = \rho(tr) > \rho(t)$

โดยการอุปมานสมมุติฐานข้างต้นกับ r และ t เราได้

$r = up_1^{\alpha_1 \cdots} p_n^{\alpha_n}$

และ $t = vq_1^{\beta_1 \cdots} q_m^{\beta_m}$

โดยที่ u และ v เป็น unit p_i's และ q_i's เป็นจำนวนเฉพาะ

แล้ว $s = (uv)p_1^{\alpha_1 \cdots} p_n^{\alpha_n} q_1^{\beta_1 \cdots} q_m^{\beta_m}$

ข้อพิสูจน์สมบูรณ์

จะพิสูจน์ uniqueness เราทำโดยใช้การอุปมานบน $\rho(x)$; $x \in R$

ถ้า $x \in R$ โดยที่ $\rho(x) \leqslant \rho(r)$ สำหรับทุก ๆ $r \in R \setminus \{0\}$

แล้ว x เป็น unit และทฤษฎีเป็นจริง

สมมติว่า ทุก ๆ $r \in R$ ซึ่ง $\rho(1) \leqslant \rho(r) < k$ สามารถจะแยก (ตัวประกอบ) เป็นได้อย่างเดียว (uniquely)

ให้ $s \in R$ โดยที่ $\rho(s) = k$

ให้ $s = up_1^{\alpha_1 \cdots} p_n^{\alpha_n} = vq_1^{\beta_1 \cdots} q_m^{\beta_m}$ โดยที่ u และ v เป็น unit และ p_i's, q_i's เป็น จำนวนเฉพาะโดยที่ไม่มี p_i เป็น associate ของ p_j สำหรับ $i \neq j$ และไม่มี q_i เป็น associate ของ q_j สำหรับ $i \neq j$

$\therefore\ p_1 | s$

$\therefore\ p_1 | (vq_1 \cdots q_m)$

โดยบทแทรกของทฤษฎี 7.3.5

$p_1 | q_i$ สำหรับบาง i

แต่ q_i เป็นจำนวนเฉพาะ

ดังนั้น p_1 และ q_i เป็น associate

$\therefore\ q_i = wp_1$ โดยที่ w เป็น unit

$\therefore\ up_1^{\alpha_1} \cdots p_n^{\alpha_n} = p_1(up_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n})$

และ $vq_1^{\beta_1} \cdots q_m^{\beta_m} = q_i(vq_1^{\beta_1} \cdots q_i^{\beta_i - 1} \cdots q_m^{\beta_m})$

$= p_1(wvq_1^{\beta_1} \cdots q_i^{\beta_i - 1} \cdots q_m^{\beta_m})$

ด้วยเหตุนี้

$up_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n} = vwq_1^{\beta_1} \cdots q_i^{\beta_i - 1} \cdots q_m^{\beta_m}$

โดยทฤษฎี 7.3.8 เราได้

$\rho(up_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n}) < k$

และข้อพิสูจน์สมบูรณ์โดยการอุปมานสมมติฐาน

แบบฝึกหัดที่ 7

1) จงพิจารณาข้อความแต่ละข้อต่อไปนี้เป็นจริงหรือเท็จ

...............ก) $x - 2$ เป็นพหุนามลดทอนไม่ได้ เหนือ Q

..............ข) $3x - 6$ เป็นพหุนามลดทอนไม่ได้ เหนือ Q

..............ค) $x^2 - 3$ เป็นพหุนามลดทอนไม่ได้ เหนือ Q

..............ง) $x^2 + 3$ เป็นพหุนามลดทอนไม่ได้ เหนือ Z_7

..............จ) ถ้า F เป็นสนามแล้ว unit ของ $F[x]$ คือ สมาชิกตัวที่ไม่ใช่ 0 ของ F

..............ฉ) พหุนาม $f(x)$ ที่มีลำดับขั้น n และมีสัมประสิทธิ์อยู่ในสมการ F จะมีศูนย์ใน F ได้มากที่สุด n ตัว

..............ช) พหุนาม $f(x)$ ที่มีลำดับขั้น n และมีสัมประสิทธิ์อยู่ในสนาม F จะมีศูนย์ในสนาม E ใด ๆ ซึ่ง $F \leqslant E$ ได้อย่างมากที่สุด n ตัว

..............ซ) ทุก ๆ กลุ่มอุดมคติของ $F[x]$ เป็นกลุ่มอุดมคติหลัก

..............ฌ) ทุก ๆ กลุ่มอุดมคติหลักใน $F[x]$ เป็นกลุ่มอุดมคติใหญ่สุด

2) ให้ $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ และ $g(x) = x^2 + 2x - 3$ เป็นพหุนามใน $Z_7[x]$ จงหา $q(x)$ และ $r(x)$ ใน $Z_7[x]$ ซึ่งทำให้ $f(x) = g(x)\,q(x) + r(x)$ โดยที่ $\deg(r(x)) < 2$

3) ให้ $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ และ $g(x) = 3x^2 + 2x - 3$ เป็นพหุนามใน $Z_7[x]$ จงหา $q(x)$ และ $r(x)$ ใน $Z_7[x]$ ซึ่งทำให้ $f(x) = g(x)\,q(x) + r(x)$ โดยที่ $\deg(r(x)) < 2$

4) พหุนาม $x^4 + 4$ สามารถแยกตัวประกอบออกมาได้เป็นผลคูณของตัวประกอบลำดับขั้นหนึ่ง (linear factor) ใน $Z_5[x]$ จงหาตัวประกอบเหล่านั้น

5) พหุนาม $x^3 + 2x + 3$ เป็นพหุนามลดทอนไม่ได้ใน $Z_5[x]$ ใช่หรือไม่ ทำไม? จงเขียนผลคูณของพหุนามลดทอนไม่ได้นี้ใน $Z_5[x]$

6) จงแสดงว่า $f(x) = x^2 + 8x - 2$ เป็นพหุนามลดทอนไม่ได้ เหนือ Q

7) พหุนามในข้อ 6 เป็นพหุนามลดทอนไม่ได้เหนือ R หรือไม่? ทำไม?

8) พหุนามในข้อ 6 เป็นพหุนามลดทอนไม่ได้เหนือ C หรือไม่? ทำไม?