บทที่ 6

ยูคลิเดียนโดเมน
(Euclidean Domain)

ในบทนี้จะศึกษาเกี่ยวกับเรื่องของอินติกรัลโดเมน ที่เรียกว่ายูคลิเดียนโดเมน และตัวอย่างอันหนึ่งของยูคลิเดียนโดเมน คือ โดเมนของจำนวนเต็มเกาส์เซี่ยน (Gaussian Integer)

ก่อนที่จะศึกษาเรื่องดังกล่าว จะกล่าวถึงการหาร และตัวหารร่วมมากในอินติกรัล-โดเมน

6.1. การหารในอินติกรัลโดเมน

นิยาม 6.1.1 ถ้า $a \neq 0$ และ b เป็นสมาชิกของอินติกรัลโดเมน D จะเรียกว่า a หาร b ลงตัว ก็ต่อเมื่อมีสมาชิก c ของ D ซึ่ง $b = ac$

สัญลักษณ์ a หาร b ลงตัว จะใช้สัญลักษณ์แทนด้วย a/b

a หาร b ไม่ลงตัว จะใช้สัญลักษณ์แทนด้วย $a \nmid b$

จากนิยามนี้ อาจจะกล่าวได้ว่า ถ้า a/b ก็คือ a เป็นตัวร่วม (factor) ของ b หรือกล่าวว่า b ถูกหารด้วย a หรือ b เป็นผลคูณของ a

ทฤษฎี 6.1.1 ให้ a, b, c เป็สมาชิกในอินติกรัลโดเมน D จะได้ว่า

1. ถ้า a/b แล้วจะได้ว่า ac/bc
2. ถ้า a/b และ b/c แล้วจะได้ว่า a/c

3. ถ้า c/a และ c/b แล้วจะได้ว่า $c/ax + by$ สำหรับทุกๆ $x, y \in D$

<u>พิสูจน์</u> 1. เนื่องจาก a/b นั่นคือจะมีสมาชิก $x \in D$ ซึ่ง $b = ax$

ดังนั้น $bc = (ax)c$

$= (ac)x$ สำหรับ $x \in D$

แสดงว่า ac/bc

2. เนื่องจาก a/b และ b/c นั่นคือจะมีสมาชิก $x, y \in D$ ซึ่ง $b = ax$ และ $c = by$

$c = (ax)y$

$= a(xy)$ สำหรับ $xy \in D$

แสดงว่า a/c

3. เนื่องจาก c/a ดังนั้นจะมีสมาชิก $p \in D$ ซึ่ง $a \in cp$

ดังนั้น $ax = (cp)x$ สำหรับสมาชิก $x \in D$

และเนื่องจาก c/b ดังนั้นจะมีสมาชิก $q \in D$ ซึ่ง $b = cq$

ดังนั้น $by = (cq)y$ สำหรับสมาชิก $y \in D$

จะได้ $ax + by = (cp)x + (cq)y$

$= c(px) + c(qy)$

$= c(px + qy)$

นั่นคือ $c/ax + by$ สำหรับทุกๆสมาชิก $x, y \in D$

<u>นิยาม 6.1.2</u> ให้ a เป็นสมาชิกของอินติกรัลโดเมน D โดย $a \neq 0$ จะเรียก a ว่าเป็นยูนิต (Unit) ของ D ก็ต่อเมื่อมีสมาชิก b ที่อยู่ใน D ซึ่ง $ab = e$ นั่นคือ a จะเป็นยูนิตในอินติกรัลโดเมน D ก็ต่อเมื่อ a มีอินเวอร์สสำหรับการคูณอยู่ใน D

<u>นิยาม 6.1.3</u> ให้ a และ b เป็นสมาชิกในอินทิกรัลโดเมน D จะเรียกว่า a และ b เป็นสมาชิกสัมพันธ์ (associated elements) ถ้า b = ua โดยที่ u เป็นยูนิตใน D

<u>ตัวอย่าง 6.1.1</u> ในริงของจำนวนเต็ม I จะมี 1 และ −1 เป็นยูนิต ดังนั้นสมาชิกสัมพันธ์ของ 26 คือ 26 และ −26 เพราะว่า $26 = (1)(26)$ และ $26 = (-1)(-26)$

<u>ทฤษฎี 6.1.2</u> ให้ $a \neq 0, b \neq 0$ เป็นสมาชิกของอินทิกรัลโดเมน D จะได้ว่า a และ b เป็นสมาชิกสัมพันธ์กัน ก็ต่อเมื่อ a/b และ b/a

<u>พิสูจน์</u> <u>ตอนแรก</u> สมมุติให้ a และ b เป็นสมาชิกสัมพันธ์กันจะพิสูจน์ว่า a/b และ b/a

จะได้ว่า $a = ub$ เมื่อ u เป็นยูนิตใน D

และ $b = u^{-1}a$ เมื่อ u^{-1} อยู่ใน D

นั่นคือ a/b และ b/a

<u>ตอนสอง</u> สมมุติให้ a/b และ b/a จะพิสูจน์ว่า a และ b เป็นสมาชิกสัมพันธ์กัน

เนื่องจาก a/b และ b/a

ดังนั้น $b = ax$ สำหรับบางสมาชิก $x \in D$

และ $a = by$ สำหรับบางสมาชิก $y \in D$

จะได้ว่า
$$b = (by)x$$
$$= b(yx)$$

หรือ $be = b(yx)$

โดยกฎการตัดออกสำหรับการคูณในอินทิกรัลโดเมน D และ $b \neq 0$

จึงได้ว่า $e = yx$

แสดงว่า y เป็นยูนิตใน D

และเนื่องจาก $a = by$

นั่นคือ a และ b เป็นสมาชิกสัมพันธ์

6.2. ตัวหารร่วมมากในอินติ รัลโดเมน

(Greatest Common Divisor in Integral Domain)

นิยาม 6.2.1 ถ้า $a \neq 0, b \neq 0$ เป็นสมาชิกของอินทิกรัลโดเมน D แล้วสมาชิก $d \in D$ จะเรียกว่าตัวหารร่วมมาก (greatest common divisor) ซึ่งจะเขียนแทนด้วย ห.ร.ม. หรือ g.c.d ของ a และ b ก็ต่อเมื่อ

1. d/a และ d/b
2. ถ้ามี c/a และ c/b แล้วจะได้ว่า c/d

ตัวอย่าง 6.2.1 ให้ I เป็นอินทิกรัลโดเมนของจำนวนเต็ม พิจารณา $8, 12 \in I$ จะมี $4 \in I$ ซึ่ง

1. 4/8 และ 4/12
2. และมี 2/8 และ 2/12 แล้วจะได้ว่า 2/4

แสดงว่า 4 เป็น ห.ร.ม. ของ 8 และ 12

นิยาม 6.2.2 ถ้า $a_1, a_2, \ldots\ldots\ldots, a_n$ เป็นสมาชิกที่ไม่ใช่ศูนย์ของอินทิกรัลโดเมน D จะกล่าวว่า สมาชิก $d \in D$ เป็นตัวหารร่วมมากของ $a_1, a_2, \ldots\ldots, a_n$ ก็ต่อเมื่อ

1. d/a_i สำหรับ $i = 1, 2, \ldots\ldots, n$
2. ถ้า c/a_i สำหรับ $i = 1, 2, \ldots\ldots, n$ แล้วจะได้ c/d

สัญลักษณ์ ถ้าเขียนว่า $d = (a_1, a_2, \ldots\ldots, a_n)$ หมายความว่า d เป็น ห.ร.ม.ของ $a_1, a_2, \ldots\ldots, a_n$

หมายเหตุ ห.ร.ม. ของ $a_1, a_2, \ldots\ldots, a_n \in D$ จะมีได้เพียงตัวเดียวเท่านั้น เพราะว่า ถ้าสมมุติให้ d และ d' ต่างก็เป็น ห.ร.ม. ของ $a_1, a_2, \ldots\ldots, a_n$ โดยที่ $d \neq d'$ จากนิยาม 6.2.2 d/d' และ d'/d แสดงว่า $d = d'$ ซึ่งเกิดการขัดแย้งขึ้น

6.3 ยูคลิเดียนโดเมน

นิยาม 6.3.1 ยูคลิเดียนเวลูเอชัน (Euclidean Valuation) บนอินทิกรัลโดเมน D หมายถึงฟังก์ชัน ν ซึ่งจะส่งสมาชิกที่ไม่ใช่ศูนย์ของ D ไปยังจำนวนเต็มที่ไม่เป็นลบ โดยสอดคล้องคุณสมบัติดังนี้

1. สำหรับทุกๆสมาชิก $a, b \in D$ ซึ่ง $b \neq 0$ จะมี q, r ใน D ซึ่ง $a = bq + r$ โดยที่ $r = 0$ หรือ $\nu(r) < \nu(b)$

2. สำหรับทุกๆสมาชิก $a, b \in D$ ซึ่งทั้ง $a \neq 0$ และ $b \neq 0$ ได้ว่า $\nu(a) \leq \nu(ab)$

นิยาม 6.3.2 จะเรียกอินทิกรัลโดเมน D ว่า ยูคลิเดียนโดเมนก็ต่อเมื่อมียูคลิเดียนเวลูเอชัน บน D

ตัวอย่าง 6.3.1 พิจารณาอินทิกรัลโดเมน I จะแสดงว่า I เป็นยูคลิเดียนโดเมน

กำหนดฟังก์ชัน $\nu : I \dashrightarrow I^+ \cup \{0\}$ เมื่อ I^+ คือเซ็ตของจำนวนเต็มบวก

โดย $\nu(n) = |n|$ เมื่อ $n \in I$ และ $n \neq 0$

จะเห็นว่าสำหรับ $n \neq 0$ ใดๆใน I นั้น $\nu(n)$ จะเป็นจำนวนเต็มที่ไม่เป็นลบเสมอ และโดยอาศัยดิวิชันอัลกอริทึมในเซ็ตของจำนวนเต็ม จะได้ว่าคุณสมบัติข้อ 1 ในนิยาม 6.3.1 จะเป็นจริงเสมอในเซ็ต I

เนื่องจาก $|n| \leq |nm|$ สำหรับจำนวนเต็ม $n \neq 0$, $m \neq 0$

นั่นคือ $\nu(n) \leq \nu(nm)$

ดังนั้น I เป็นยูคลิเดียนโดเมน

ทฤษฎี 6.3.1 ถ้า A เป็นไอดีลของยูคลิเดียนโดเมน D จะได้ว่ามีสมาชิก $a_0 \in A$ ซึ่งทำให้สมาชิกที่อยู่ใน A เขียนได้ในรูป $a_0 r$ โดยที่ r เป็นสมาชิกของ D

<u>พิสูจน์</u> <u>กรณีที่ 1</u> ถ้า A มีสมาชิกศูนย์เพียงตัวเดียว นั่นคือ $A = \{0\}$

ให้ $a_o = 0$

ดังนั้น $A = \{0r \,/\, r \in D\}$

$= (0)$

แสดงว่าหฤษฎีเป็นจริงในกรณี $A = \{0\}$

<u>กรณีที่ 2</u> ถ้า $A \neq \{0\}$

ดังนั้นจะมีสมาชิก a ที่ไม่ใช่ศูนย์อยู่ใน A

เลือก $a_o \in A$ โดยที่ $\mathcal{V}(a_o)$ มีค่าน้อยที่สุด

ให้ $a \in A$

พิจารณา $a, a_o \in A$

จากนิยาม 6.3.1 ข้อ 1 จะได้ว่ามี $t, r \in D$ ซึ่ง

$$a = ta_o + r \qquad \text{โดยที่ } r = 0 \text{ หรือ } \mathcal{V}(r) < \mathcal{V}(a_o)$$

เนื่องจาก $a_o \in A$ และ A เป็นไอดีลของ D

จะได้ $ta_o \in A$ สำหรับ $t \in D$

ดังนั้น $a - ta_o \in A$

แต่ $r = a - ta_o$

นั่นคือ $r \in A$

ถ้า $r \neq 0$ แสดงว่า $\mathcal{V}(r) < \mathcal{V}(a_o)$

ซึ่งจะขัดแย้งกับที่ว่า $a_o \in A$ โดยที่ $\mathcal{V}(a_o)$ มีค่าน้อยที่สุด

ดังนั้น $r = 0$ ซึ่งจะทำให้ $a = ta_o = a_ot$ โดยที่ $t \in D$

<u>ทฤษฎี 6.3.2</u> ให้ D เป็นยูคลิเดียนโดเมน และ $a, b \in D$ ถ้า b ไม่ใช่ยูนิตใน D แล้ว จะได้ว่า $\nu(a) < \nu(ab)$

<u>พิสูจน์</u> พิจารณา $A = (a) = \{ra / r \in D\}$ ซึ่งเป็นไอดีลของ D จากนิยาม 6.3.1 ข้อ 2 จะได้ว่า

$\nu(a) \leq \nu(ra)$ เมื่อ $r \neq 0$

นั่นคือ $\nu(a) \leq \nu(ab)$

เนื่องจาก $ab \in A$

สมมุติว่า $\nu(a) = \nu(ab)$

จากการพิสูจน์ทฤษฎี 6.3.1 จะได้ว่าทุกๆ สมาชิกใน A เป็นผลคูณของ ab

เนื่องจาก $a \in A$ ดังนั้น a จะเป็นผลคูณของ ab

นั่นคือ $a = (ab)r$ สำหรับบางสมาชิก $r \in D$

หรือ $ae = a(br)$

โดยกฎการตัดออกสำหรับการคูณในอินทิกรัลโดเมน

จะได้ $e = br$

แสดงว่า b เป็นยูนิตใน D ซึ่งจะขัดแย้งกับที่ว่า b ไม่ใช่ยูนิตใน D

นั่นคือ $\nu(a) \neq \nu(ab)$

แสดงว่า $\nu(a) < \nu(ab)$

<u>ทฤษฎี 6.3.3</u> ให้ D เป็นยูคลิเดียนโดเมน โดยมี ν เป็นยูคลิเดียนเวลูเอชันจะได้ว่า

1. สำหรับแต่ละสมาชิก $a \in D$ และ $a \neq 0$, $\nu(a) \geq \nu(e)$
2. ถ้า $a, b \in D$ และ $a \neq 0$, $b \neq 0$ และ a, b เป็นสมาชิกสัมพันธ์กันแล้วจะได้ $\nu(a) = \nu(b)$
3. สำหรับสมาชิก $u \in D$ ซึ่ง $u \neq 0$, u จะเป็นยูนิตก็ต่อเมื่อ

$$\nu(u) = \nu(e)$$

<u>พิสูจน์</u> 1. ให้ $a \in D$ และ $a \neq 0$

เนื่องจาก $a = ae$

ดังนั้น $\nu(a) = \nu(ae)$

จากนิยาม 6.3.1 จะได้ว่า $\nu(ae) \geq \nu(e)$

นั่นคือ $\nu(a) \geq \nu(e)$ สำหรับทุกๆสมาชิก $a \neq 0 \in D$

2. ให้ $a, b \in D$ ซึ่ง $a \neq 0$, $b \neq 0$ และ a, b เป็นสมาชิกสัมพันธ์

ดังนั้น $b = ua$ เมื่อ u คือยูนิตใน D

และจากนิยาม 6.3.1 จะได้ $\nu(b) = \nu(ua) \geq \nu(a)$ ......(ก)

แต่ $a = u^{-1}b$

ดังนั้น $\nu(a) = \nu(u^{-1}b) \geq \nu(b)$ ......(ข)

จาก ...(ก) และ ...(ข) จะได้ว่า $\nu(a) = \nu(b)$

3. <u>ตอนแรก</u> สมมุติว่า u เป็นยูนิต จะแสดงว่า $\nu(u) = \nu(e)$

เนื่องจาก $uu^{-1} = e$

ดังนั้น $\nu(uu^{-1}) = \nu(e) \geq \nu(u)$

และจากข้อ 1 $\nu(u) \geq \nu(e)$

นั่นคือ $\nu(u) = \nu(e)$

<u>ตอนสอง</u> สมมุติ $u \neq 0 \in D$ ซึ่ง $\nu(u) = \nu(e)$

เนื่องจาก $u, e, \in D$ และจากนิยาม 6.3.1 จะมี $q, r \in D$ ซึ่ง

$e = uq + r$ โดยที่ $r = 0$ หรือ $\nu(r) < \nu(u)$

ถ้า $\nu(r) < \nu(u)$

เนื่องจาก $\nu(u) = \nu(e)$

จะได้ว่า $\nu(r) < \nu(e)$ ซึ่งจะขัดแย้งกับข้อ 1 ที่ว่า $\nu(e) \leq \nu(a)$

สำหรับทุกๆ $a \in D$, $a \neq 0$

ดังนั้น $r = 0$

จะได้ว่า $e = uq$

นั่นคือ u เป็นยูนิตใน D

<u>ทฤษฎี 6.3.4</u> ให้ D เป็นยูคลิเดียนโดเมน มี ν เป็นยูคลิเดียนเวลูเอชัน ถ้า a, b เป็นสมาชิกใน D โดยที่ $a \neq 0, b \neq 0$ แล้วจะมี ห.ร.ม. ของ a และ b ซึ่งสามารถเขียนได้ในรูป $\lambda a + \mu b$ สำหรับบางสมาชิก $\lambda, \mu \in D$

<u>พิสูจน์</u> ให้ $N = \{ra + sb \,/\, r, s \in D\}$

จะแสดงว่า N เป็นไอดีลของ D

เนื่องจาก $a, b, r, s \in D$ จะได้ว่า $ra + sb \in D$ $N \subseteq D$

และเนื่องจาก $0, e \in D$ จะได้ว่า $0.a + eb = b \in N$ นั่นคือ $N \neq \emptyset$

ให้ $x, y \in N$

ดังนั้น $x = r_1a + s_1b$ สำหรับ $r_1, s_1 \in D$

และ $y = r_2a + s_2b$ สำหรับ $r_2, s_2 \in D$

พิจารณา $x - y = (r_1a + s_1b) - (r_2a + s_2b)$

$= (r_1 - r_2)a + (s_1 - s_2)b$ ซึ่ง $r_1 - r_2$ และ $s_1 - s_2 \in D$

และ $xy = (r_1a + s_1b)(r_2a + s_2b)$

$= r_1ar_2a + s_1br_2a + r_1as_2b + s_1bs_2b$

$= (r_1r_2a + s_1br_2)a + (r_1as_2 + s_1bs_2)b$

ซึ่ง $(r_1r_2a + s_1br_2), (r_1as_2 + s_1bs_2) \in D$

ดังนั้น $x - y$ และ $xy \in N$

นั่นคือ N เป็นสับริงของ D

ให้ $x \in N$ และ $d \in D$

ดังนั้น $x = r_1a + s_1b$ สำหรับ $r_1, s_1 \in D$

พิจารณา $dx = d(r_1a + s_1b)$

$= dr_1a + ds_1b$ ซึ่ง $dr_1, ds_1 \in D$

ดังนั้น $dx \in N$

และเนื่องจาก D เป็นคอมมิวเทที่พริง ดังนั้น $xd = dx \in N$

นั่นคือ N เป็นไอดีลของ D

จากทฤษฎี 6.3.1 จะมี $a_o \in N$ ซึ่ง $N = (a_o)$

นั่นคือทุกๆสมาชิกใน N เขียนเป็นผลคูณของ a_o ได้

ดังนั้น $a_o / ra + sb$ สำหรับทุกๆ สมาชิก $r, s \in D$

ถ้าให้ $s = 0, r = e$ จะได้ $a_o / ea + 0b$ หรือ a_o / a

และถ้าให้ $s = e, r = 0$ จะได้ $a_o / 0a + eb$ หรือ a_o / b

สมมุติให้ c/a และ c/b

จากทฤษฎี 6.1.1 จะได้ว่า $c/r\ a + sb$ สำหรับทุกๆสมาชิก $r, s \in D$

นั่นคือ c/n สำหรับทุกสมาชิก $n \in N$

ดังนั้น c/ a_o

แสดงว่า a_o เป็น ห.ร.ม. ของ a และ b

เนื่องจาก $a_o \in N$ ดังนั้น $a_o = \lambda a + \mu b$ สำหรับบาง $\lambda, \mu \in D$

<u>ทฤษฎี 6.3.5</u> (Euclidean Algorithm)

ให้ D เป็นยูคลิเดียนโดเมนที่มี ν เป็นยูคลิเดียนเวลูเอชัน และให้ a, b เป็นสมาชิกของ D โดยที่ $a \neq 0$, $b \neq 0$ ให้ r_1 เป็นสมาชิกใน D ซึ่งสอดคล้อง

$a = bq_1 + r_1$ ซึ่ง $r_1 = 0$ หรือ $\nu(r_1) < \nu(b)$

ถ้า $_1 \neq 0$ ให้ r_2 เป็นสมาชิกใน D ซึ่ง

$b = r_1 q_2 + {}_2$ ซึ่ง $r_2 = 0$ หรือ $\nu(r_2) < \nu(r_1)$

โดยทั่วๆไปให้ r_{i+1} เป็นสมาชิกใน D ซึ่งสอดคล้อง

$r_{i-1} = r_i q_{i+1} + r_{i+1}$ ซึ่ง $r_{i+1} = 0$

หรือ $\nu(r_{i+1}) < \nu(r_i)$

จะได้ว่าในอันดับ $r_1, r_2, \ldots\ldots\ldots$ จะต้องสิ้นสุดลงที่ r_i ตัวหนึ่งสมมุติเป็น $r_s = 0$ ถ้า $r_1 = 0$ แล้ว b จะเป็น ห.ร.ม. ของ a และ b ถ้า $r_1 \neq 0$ และ r_s คือ r_i ตัวแรกที่เท่ากับ 0 แล้ว ห.ร.ม.ของ a และ b คือ r_{s-1}

<u>พิสูจน์</u> เนื่องจาก $\nu(r_i) < \nu(r_{i-1})$ และ $\nu(r_i)$ เป็นจำนวนเต็มที่ไม่เป็นลบ

จะได้ว่า จะมีบาง r_s ซึ่ง $r_s = 0$

ถ้า $r_1 = 0$ ดังนั้น $a = bq_1$

นั่นคือ b เป็น ห.ร.ม. ของ a และ b

สมมุติ $r_1 \neq 0$ ถ้า d/a และ d/b จะได้ $d/ a - bq_1$

ดังนั้น d/r_1

และถ้า d_1 / r_1 และ d_1 / b จะได้ $d_1 / bq_1 + r_1$

ดังนั้น d_1 / a

นั่นคือเซ็ตของตัวหารร่วมของ a และ b จะเป็นเซ็ตเดียวกันกับเซ็ตของตัวหารร่วมของ b และ r_1

ในทำนองเดียวกัน ถ้า $r_2 \neq 0$ จะได้ว่าเซ็ตของตัวหารร่วมของ b และ r_1 จะเป็นเซ็ตเดียวกันกับเซ็ตของตัวหารร่วมของ r_1 และ r_2

โดยวิธีเดียวกันนี้ กระทำไปเรื่อยๆในที่สุด จะได้ว่าเซ็ตของตัวร่วมของ a และ b เป็นเซ็ตเดียวกันเกับเซ็ตของตัวหารร่วมของ r_{s-2} และ r_{s-1} ซึ่ง r_s เป็น r_i ตัวแรกที่เท่ากับศูนย์

ดังนั้น ห.ร.ม.ของ r_{s-2} และ r_{s-1} เป็น ห.ร.ม.ของ a และ b ด้วย

แต่จากสมการ
$$r_{s-2} = q_s r_{s-1} + r_s$$
$$= q_s r_{s-1}$$

แสดงว่า ห.ร.ม. ของ r_{s-2} และ r_{s-1} คือ r_{s-1}

ดังนั้น ห.ร.ม. ของ a , b คือ r_{s-1} เมื่อ r_s เป็น r_i ตัวแรกที่เท่ากับศูนย์

<u>ตัวอย่าง 6.3.2</u> แสดงการใช้ยูคลิเดียนอัลกอริทึมสำหรับยูคลิเดียนเวลูเอชันที่กำหนดไว้ใน ตัวอย่าง 6.3.1 บนยูคลิเดียนโดเมน I โดยการคำนวณหา ห.ร.ม.ของ 22,471 และ 3,266

$22,471 = (3,266)6 + 2,875 \quad r_1 = 2,875$ โดยที่ $|2,875| < |3,266|$

$3,266 = (2,875) + 391 \quad r_2 = 391$ โดยที่ $|391| < |2,875|$

$2,875 = (391)7 + 138 \quad r_3 = 138$ โดยที่ $|138| < |291|$

$391 = (138)2 + 115 \quad r_4 = 115$ โดยที่ $|115| < |138|$

$138 = (115)1 + 23 \quad r_5 = 23$ โดยที่ $|23| < |115|$

$115 = (23)5 + 0 \quad r_6 = 0$

ดังนั้น $r_5 = 23$ คือ ห.ร.ม. ของ 22,471 และ 3,266

<u>ตัวอย่าง 6.3.3</u> จากนิยาม 6.3.1 ข้อ 1 ไม่ได้บังว่า r_i จะต้องเป็นจำนวนบวก ดังนั้นในการคำนวณ ห.ร.ม. ในเซ็ต I โดยใช้ยูคลิเดียนอัลกอริทึม สำหรับยูคลิเดียน-เวลูเอชันในตัวอย่าง 6.3.1 จึงสามารถทำให้ r_i เล็กเท่าไรก็ได้ในการหารแต่ละครั้ง ดังนั้นตัวอย่าง 6.3.2 อาจจะกระทำได้ใหม่ดังนี้

$$a = 22,471, \quad b = 3,266$$

$22,471 = (3,266)7 - 391 \quad r_1 = -391$ โดยที่ $|-391| < |3,266|$

$3,266 = (391)8 + 138 \quad r_2 = 138$ โดยที่ $|138| < |-391|$

$391 = (138)3 - 23 \quad r_3 = -23$ โดยที่ $|-23| < |138|$

$138 = (23)6 + 0 \quad r_4 = 0$

ดังนั้น ห.ร.ม. ของ 22,471 และ 3,266 คือ 23

<u>หมายเหตุ</u> สามารถเปลี่ยนเครื่องหมายของ r_i จากลบเป็นบวกได้ เพราะว่าตัวหารของ r_i และ $-r_i$ เป็นตัวเดียวกัน

แบบฝึกหัด 6 ก

1. ให้ x , y , z , t เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์ ซึ่ง $x = yz + t$, จงแสดงว่า $(x , z) = (z , t)$
   [(x, z) หมายถึง ห.ร.ม. ของ x และ z]
2. ให้ D เป็นอินทิกรัลโดเมน จงพิสูจน์ว่าสำหรับ a , b , c ที่ไม่เป็นศูนย์ใน D
   - ก. $(a , (b , c)) = ((a , b) , c)$
   - ข. $(a , 1) = 1$
   - ค. $(ca , cb) = c(a , b)$ ในกรณีเฉพาะ $(c , cb) = 1$
   - ง. ถ้า $(a , b) = 1$ และ $(a , c) = 1$ แล้วจะได้ $(a , bc) = 1$
   - จ. ถ้า $(a , b) = 1$, a/c และ b/c แล้วจะได้ ab/c
3. ในคอมมิวเทฟริงที่มียูนิตี้ จงพิสูจน์ว่าความสัมพันธ์(relation) ที่ว่า a และ b เป็นสมาชิกสัมพันธ์กัน เป็นความสัมพันธ์สมมูลย์ (Equivalence relation)
4. จงพิสูจน์ว่า เซ็ตของยูนิตในคอมมิวเทฟริงที่มียูนิตี้ เป็นอบีเลี่ยนกรุ๊ป
5. กำหนดให้สมาชิก 2 ตัว คือ a , b ในยูคลิเดียนโดเมน D มี c เป็น ค.ร.น อยู่ใน D ซึ่ง a/c และ b/c และเมื่อไรก็ตาม a/x และ b/x สำหรับ $x \in D$ แล้ว c/x จงพิสูจน์ว่าสมาชิก 2 ตัวใดๆ ในยูคลิเดียนโดเมน D จะมี ค.ร.น อยู่ใน D
6. ในข้อ 6 ถ้า ค.ร.น. ของ a และ b เขียนแทนด้วย $\{a , b\}$ จงพิสูจน์ว่า

$$\{a , b\} = \frac{ab}{(a , b)}$$

7. จงบอกว่าฟังก์ชัน ν ต่อไปนี้ ฟังก์ชันใดเป็นยูคลิเดียนเวลูเอชัน สำหรับอินทิกรัลโดเมนที่กำหนดให้

ก. ฟังก์ชัน ν ของ I กำหนดโดย $\nu(n) = n^2$ สำหรับ $n \neq 0 \in I$

ข. ฟังก์ชัน ν สำหรับ $I[x]$ กำหนดโดย $\nu(f(x)) =$ (degree ของ $f(x)$) สำหรับ $f(x)$ ที่ไม่ใช่ศูนย์ใน $I[x]$

ค. ฟังก์ชัน ν สำหรับเซ็ตของจำนวนตรรกยะ Q โดย $\nu(a) = a^2$ สำหรับ $a \neq 0 \in Q$

ง. ฟังก์ชัน ν สำหรับ Q โดย $\nu(a) = 50$ สำหรับ $a \neq 0 \in Q$

8. จงหา ห.ร.ม. ของ 49 , 349 และ 15, 555 ใน I

9. $I[x]$ เป็นยูคลิเดียนโดเมน หรือไม่เพราะเหตุใด

10. จงแสดงว่า $\{a + xf(x) / a \in 2I,\ f(x) \in I[x]\}$ เป็นไอดีลใน $I[x]$

11. จงแสดงว่า ถ้า $s \in I$ ซึ่ง $s + \nu(e) > 0$ แล้ว $\eta : D^* \longrightarrow I$ โดย $\eta(a) = \nu(a) + s$ สำหรับ $a \neq 0 \in D$ เป็นยูคลิเดียนเวลูเอชันใน D

D^* เป็นเซ็ตของสมาชิกที่ไม่ใช่ศูนย์ของ D , ν คือ ยูคลิเดียนเวลูเอชันในยูคลิเดียนโดเมน D

12. จงแสดงว่าสำหรับ $r \in I^+$, $\lambda : D^* \longrightarrow I$ โดย $\lambda(a) = r(\nu(a))$ สำหรับ a ซึ่งไม่ใช่ศูนย์ใน D เป็นยูคลิเดียนเวลูเอชันใน D , D^* และ ν เหมือนข้อ 11

13. ถ้า u_o เป็นยูนิตในอินทิกรัลโดเมน D และ $U = (u_o)$ เป็นไอดีลใน D แล้ว จงแสดงว่า $U = D$

6.4 จำนวนเต็มเกาส์เซี่ยนและนอร์ม (Gaussian Integers and Norm)

ในหัวข้อนี้จะกล่าวถึงเซ็ตของจำนวนเต็มเกาส์เซี่ยน ซึ่งเป็นตัวอย่างหนึ่งของยูคลิเดียนโดเมน

<u>นิยาม 6.4.1</u> จำนวนเต็มเกาส์เซี่ยน คือ จำนวนเชิงซ้อน $a + bi$ ซึ่ง $a , b \in I$

<u>สัญลักษณ์</u> เขียน $I(i)$ แทนเซ็ตของจำนวนเต็มเกาส์เซี่ยนทั้งหมด

<u>นิยาม 6.4.2</u> สำหรับจำนวนเต็มเกาส์เซี่ยน $\alpha = a + bi$ นอร์มของ α ซึ่งเขียนแทนด้วย $N(\alpha)$ คือ $a^2 + b^2$

<u>เล็มมา 6.4.1</u> ในเซ็ตของจำนวนเต็มเกาส์เซี่ยน $I(i)$ คุณสมบัติของนอร์มต่อไปนี้จะเป็นจริงสำหรับทุกๆสมาชิก $\alpha , \beta \in I(i)$

1. $N(\alpha) \geq 0$
2. $N(\alpha) = 0$ ก็ต่อเมื่อ $\alpha = 0$
3. $N(\alpha\beta) = N(\alpha)N(\beta)$

<u>พิสูจน์</u> ให้ $\alpha , \beta \in I(i)$

ดังนั้น $\alpha = a_1 + a_2 i$ และ $\beta = b_1 + b_2 i$ สำหรับ $a_1, a_2, b_1, b_2 \in I$

1. เนื่องจาก $N(\alpha) = a_1^2 + a_2^2$ และ $a_1 , a_2 \in I$ ดังนั้น $a_1^2 \geq 0$, $a_2^2 \geq 0$

ดังนั้น $N(\alpha) = a_1^2 + a_2^2 \geq 0$

สำหรับ 2, 3 ให้ทำเป็นแบบฝึกหัด

<u>นิยาม 6.4.3</u> กำหนดการบวกและการคูณในเซ็ต $I(i)$ เหมือนกับการบวกและการคูณในเซ็ตของจำนวนเชิงซ้อน นั่นคือ สำหรับ $\alpha = a_1 + a_2 i$ และ $\beta = b_1 + b_2 i$ เป็นสมาชิกใน $I(i)$

$$\alpha + \beta = (a_1 + a_2i) + (b_1 + b_2i)$$
$$= (a_1 + b_1) + (a_2 + b_2)i$$

และ $$\alpha\beta = (a_1 + a_2i)(b_1 + b_2i)$$
$$= (a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)i$$

<u>เล็มม่า 6.4.2</u> $I(i)$ เป็นอินติกรัลโดเมนภายใต้การบวก และการคูณ

<u>พิสูจน์</u> <u>ตอนแรก</u> จะแสดงว่า $I(i)$ เป็นคอมมิวเทฑีฟริง ภายใต้การบวก และการคูณ

ใน $I(i)$

ให้ $\alpha, \beta, \gamma, \varepsilon I(i)$

ดังนั้น $\alpha = a_1 + a_2i$, $\beta = b_1 + b_2i$ และ $\gamma = c_1 + c_2i$

เมื่อ $a_1, a_2, b_1, b_2, c_1, c_2 \varepsilon I$

1. จะแสดงว่าการบวกและการคูณใน $I(i)$ เป็นไบนารีโอเปอร์เรชัน

เนื่องจาก $\alpha + \beta = (a_1 + a_2i) + (b_1 + b_2i)$ เมื่อ $a_1, a_2, b_1, b_2 \varepsilon I$

$= (a_1 + b_1) + (a_2 + b_2)i$ เมื่อ $a_1 + b_1, a_2 + b_2 \varepsilon I$

นั่นคือ $\alpha + \beta \varepsilon I(i)$

และ $\alpha\beta = (a_1 + a_2i)(b_1 + b_2i)$ เมื่อ $a_1, a_2, b_1, b_2 \varepsilon I$

$= (a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)i$

เมื่อ $a_1b_1 - a_2b_2$, $a_1b_2 + a_2b_1 \varepsilon I$

นั่นคือ $\alpha\beta \varepsilon I(i)$

แสดงว่าการบวก และการคูณนี้ เป็นไบนารีโอเปอร์เรชันบน $I(i)$

2. พิจารณา $(\alpha + \beta) + \gamma = \left[(a_1 + a_2i) + (b_1 + b_2i)\right] + (c_1 + c_2i)$

$$= \left[(a_1 + b_1) + (a_2 + b_2)i\right] + (c_1 + c_2i)$$

$$= (a_1 + b_1) + c_1 + ((a_2 + b_2) + c_2)i$$

$$= a_1 + (b_1 + c_1) + (a_2 + (b_2 + c_2))i$$

$$= (a_1 + a_2i) + \left[(b_1 + c_1) + (b_2 + c_2)i\right]$$

$$= (a_1 + a_2i) + (b_1 + b_2i) + (c_1 + c_2i)$$

$$= \alpha + (\beta + \gamma)$$

นั่นคือกฎการรวมหมู่สำหรับการบวกเป็นจริงใน I(i)

3. จะมี $0 + 0i = 0$ เป็นสมาชิกศูนย์ใน I(i) เพราะว่า

$$\alpha + 0 = (a_1 + a_2i) + (0 + 0i)$$

$$= (a_1 + 0) + (a_2 + 0)i$$

$$= a_1 + a_2i$$

$$= \alpha$$

และ $0 + \alpha = (0 + 0i) + (a_1 + a_2i)$

$$= (0 + a_1) + (0 + a_2)i$$

$$= a_1 + a_2i$$

$$= \alpha$$

4. จะมี $-\alpha = -a_1 - a_2i$ เป็นอินเวอร์สสำหรับการบวกของ α อยู่ใน I(i) เพราะว่า

$$\alpha + (-\alpha) = (a_1 + a_2i) + (-(a_1 + a_2i))$$

$$= (a_1 - a_1) + (a_2 - a_2)i$$

$$= 0 + 0i = 0$$

และ $(-\alpha) + \alpha = (-(a_1 + a_2i)) + (a_1 + a_2i)$

$$= (-a_1 + a_1) + (-a_2 + a_2)i$$

$$= 0 + 0i = 0$$

5. พิจารณา $\alpha + \beta = (a_1 + a_2i) + (b_1 + b_2i)$

$$= (a_1 + b_1) + (a_2 + b_2)i$$

$$= (b_1 + a_1) + (b_2 + a_2)i$$

$$= (b_1 + b_2i) + (a_1 + a_2i)$$

$$= \beta + \alpha$$

แสดงว่ากฎการสลับที่ สำหรับการบวกเป็นจริงใน $I(i)$

6. พิจารณา $\alpha(\beta\gamma) = (a_1 + a_2i)\ (b_1 + b_2i)(c_1 + c_2i)$

$$= (a_1 + a_2i)\left[(b_1c_1 - b_2c_2) + (b_1c_2 + b_2c_1)i\right]$$

$$= \left[(a_1(b_1c_1 - b_2c_2) - a_2(b_1c_2 + b_2c_1) + \right.$$

$$\left.\left[a_1(b_1c_2 + b_2c_1) + a_2(b_1c_1 - b_2c_2)\right] i\right.$$

$$= \left[(a_1b_1c_1 - a_1b_2c_2) - (a_2b_1c_2 + a_2b_2c_1)\right] +$$

$$\left[(a_1b_1c_2 + a_1b_2c_1 + (a_2b_1c_1 - a_2b_2c_2)\right] i$$

$$= \left[(a_1b_1 - a_2b_2)c_1 - (a_1b_2 + a_2b_1)c_2\right] +$$

$$\left[(a_1b_2 + a_2b_1)c_1 + (a_1b_1 - a_2b_2)c_2\right] i$$

$$= \left[(a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)i\right](c_1 + c_2i)$$

$$= \left[(a_1 + a_2i)(b_1 + b_2i)\right](c_1 + c_2i)$$

$$= (\alpha\beta)\gamma$$

แสดงว่ากฎการรวมหมู่ สำหรับการคูณเป็นจริงใน $I(i)$

7. พิจารณา $\alpha(\beta + \gamma) = (a_1 + a_2i)\left[(b_1 + b_2i) + (c_1 + c_2i)\right]$

$$= (a_1 + a_2i)\left[(b_1 + c_1) + (b_2 + c_2)i\right]$$

$$= \left[a_1(b_1 + c_1) - a_2(b_2 + c_2)\right] + \left[a_1(b_2 + c_2) + a_2(b_1 + c_1)\right]i$$

$$= \left[(a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)i\right] + \left[(a_1c_1 - a_2c_2) + (a_1c_2 + a_2c_1)i\right]$$

$$= (a_1 + a_2i)(b_1 + b_2i) + (a_1 + a_2i)(c_1 + c_2i)$$

$$= \alpha\beta + \alpha\gamma$$

โดยทำนองเดียวกัน จะได้ว่า $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$

นั่นคือกฎการกระจายเป็นจริงใน $I(i)$

8. พิจารณา $\alpha\beta = (a_1 + a_2i)(b_1 + b_2i)$

$$= (a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)i$$

$$= (b_1a_1 - b_2a_2) + (b_2a_1 + b_1a_2)i$$

$$= (b_1 + b_2i)(a_1 + a_2i)$$

$$= \beta\alpha$$

นั่นคือกฎการสลับที่สำหรับการคูณเป็นจริงใน $I(i)$

แสดงว่า $I(i)$ เป็นคอมมิวเทตีฟริง

และ I(i) เป็นริงที่มียูนิตี้ คือ $1 + 0.i$ หรือ 1 เพราะว่า

$$\alpha.1 = (a_1 + a_2 i)(1 + 0\, i)$$

$$= (a_1 + 0) + (a_2 + 0)i$$

$$= a_1 + a_2 i = \alpha$$

และในทำนองเดียวกันจะได้ $1.\alpha = \alpha$

ต่อไปจะแสดงว่า I(i) ไม่มีตัวหารศูนย์

ให้ $\alpha , \beta \in I(i)$ และ $\alpha\beta = 0$

จากเล็มม่า 6.4.1 ข้อ 3 จะได้ว่า $N(\alpha\beta) = N(\alpha)\, N(\beta)$

ดังนั้น $N(\alpha)\, N(\beta) = N(0)$

และจากเล็มม่า 6.4.1 ข้อ 2 จะได้ว่า $N(0) = 0$

ดังนั้น $N(\alpha)\, N(\beta) = 0$

นั่นคือ $N(\alpha) = 0$ หรือ $N(\beta) = 0$

จากเล็มม่า 6.4.1 ข้อ 2 จะได้ว่า

$\alpha = 0$ หรือ $\beta = 0$

แสดงว่า I(i) ไม่มีตัวหารศูนย์

นั่นคือ I(i) เป็นอินติกรัลโดเมน

<u>ทฤษฎี 6.4.3</u> I(i) เป็นยูคลิเดียนโดเมน

<u>พิสูจน์</u> จากเล็มม่า 6.4.2 ได้ว่า I(i) เป็นยูคลิเดียนโดเมน ดังนั้นจะต้องแสดงว่า มียูคลิเดียนเวลูเอชันบน I(i) จึงจะได้ว่า I(i) เป็นยูคลิเดียนโดเมน กำหนดฟังก์ชัน $\nu : I(i) \longrightarrow I$ โดย $\nu(\alpha) = N(\alpha)$ สำหรับสมาชิก $\alpha \neq 0$ ใน I(i)

จะแสดงว่า ν เป็นยูคลิเดียนเวลูเอชันบน $I(i)$

1. จะพิสูจน์ว่าสำหรับทุกๆสมาชิก α , β ε $I(i)$ โดยที่ $\alpha \neq 0$, $\beta \neq 0$

จะได้ว่า $N(d) \leq N(\alpha\beta)$

เนื่องจาก α , β ε $I(i)$ โดยที่ $\alpha \neq 0$, $\beta \neq 0$

ดังนั้น $\alpha = x + yi$ เมื่อ x , y ε I

จะได้ $N(\alpha) = x^2 + y^2 \geq 1$

ในทำนองเดียวกันจะได้ $N(\beta) \geq 1$

จากเล็มมา 6.4.1 ข้อ 3 จะได้ว่า

$$N(\alpha\beta) = N(\alpha)\, N(\beta)$$

ดังนั้น $N(\alpha) = N(\alpha) \cdot 1 \leq N(\alpha)\, N(\beta) = N(\alpha\beta)$

นั่นคือ $N(\alpha) \leq N(\alpha\beta)$

2. กำหนด x , y ε $I(i)$ แล้วจะต้องแสดงว่ามี t , r ε $I(i)$ ซึ่ง

$y = tx + r$ เมื่อ $r = 0$ หรือ $N(r) < N(x)$

<u>กรณีเฉพาะ</u> ให้ y เป็นสมาชิกใดๆ ใน $I(i)$ และ x เป็นจำนวนเต็มบวก n

สมมุติให้ $y = a + bi$ เมื่อ a , b ε I

จากดิวิชันอัลกอริทึมในริง I, สำหรับ a , b ε I จำนวนเต็ม u , v

$a = un + u_1$ โดยที่ $|u_1| < \frac{n}{2}$

และ $b = vn + v_1$ โดยที่ $|v_1| < \frac{n}{2}$

ให้ $t = u + vi$ และ $r = u_1 + v_1 i$

ดังนั้น $y = (un + u_1) + (vn + v_1)i$

$= (u + vi)n + (u_1 + v_1 i)$

$= tn + r$ โดยที่ $t , r \varepsilon I(i)$

พิจารณา $N(r) = N(u_1 + v_1 i)$

$= u_1^2 + v_1^2$

แต่ $u_1^2 + v_1^2 \leq \frac{n^2}{4} + \frac{n^2}{4} < n^2 = N(n)$

ดังนั้น $N(r) < N(n)$

หรือ $N(r) < N(x)$

นั่นคือ สำหรับ $x , y \varepsilon I(i)$ เมื่อ x เป็นจำนวนเต็มบวก

แล้วจะมี $t , r \varepsilon I(i)$ ซึ่ง

$y = tx + r$ เมื่อ $r = 0$ หรือ $N(r) < N(x)$

<u>กรณีทั่วไป</u> ให้ $x \neq 0$, y เป็นสมาชิกใดๆ ใน $I(i)$

ดังนั้น $x = a + bi$ และ $\bar{x} = a - bi$ เมื่อ $a , b \varepsilon I$

จะได้ว่า $x\bar{x} = a^2 + b^2$ ซึ่งเป็นจำนวนเต็มบวก

สมมุติให้ $x\bar{x} = n$

จากกรณีเฉพาะสำหรับ $y\bar{x} , n$ จะได้ว่ามี $t , r \varepsilon I(i)$ ซึ่ง

$y\bar{x} = tn + r$ เมื่อ $r = 0$ หรือ $N(r) < N(n)$

ดังนั้น $N(r) = N(y\bar{x} - tx\bar{x}) < N(n)$

แต่ $N(n) = N(x\bar{x}) = N(x) N(\bar{x})$

จะได้ $N(y\bar{x} - tx\bar{x}) < N(x) N(\bar{x})$

หรือ $N(y - tx) N(\bar{x}) < N(x) N(\bar{x})$

เนื่องจาก $x \neq 0$ ดังนั้น $N(\bar{x})$ เป็นจำนวนเต็มบวก

ดังนั้น $N(y - tx) < N(x)$

ให้ $r_o = y - tx$ นั่นคือ $y = tx + r_o$

ดังนั้นจะมี $t , r_o \in I(i)$ ซึ่ง

$$y = tx + r_o \text{ เมื่อ } r_o = 0 \text{ หรือ } N(r_o) = N(y - tx) < N(x)$$

แสดงว่า สำหรับ $x , y \in I(i)$ แล้วจะมี $t , r \in I(i)$ ซึ่ง

$$y = tx + r \quad \text{เมื่อ } r = 0 \text{ หรือ } N(r) < N(x)$$

นั่นคือ ν ซึ่งกำหนดโดย $\nu(\alpha) = N(\alpha)$ สำหรับทุกๆ $\alpha \in I(i)$

เป็นยูคลิเดียนเวลูเอชันบน $I(i)$

แสดงว่า $I(i)$ เป็นยูคลิเดียนโดเมน

6.5. <u>นอร์มของการคูณ</u> (Multiplicative Norm)

ในหัวข้อนี้จะกล่าวถึงนอร์มของการคูณ โดยจะให้นิยามและกล่าวถึงทฤษฎี ซึ่งแสดงคุณสมบัติของนอร์มของการคูณบนอินทิกรัลโดเมน

<u>นิยาม 6.5.1</u> ให้ D เป็นอินทิกรัลโดเมน จะเรียก N ว่าเป็นนอร์มของการคูณบน D ถ้า N เป็นฟังก์ชันจาก D ไปยังเซ็ตของจำนวนเต็ม I ซึ่งสอดคล้องคุณสมบัติต่อไปนี้

1. $N(\alpha) \geq 0$ สำหรับทุกๆสมาชิก $\alpha \in D$
2. $N(\alpha) = 0$ ก็ต่อเมื่อ $\alpha = 0$
3. $N(\alpha\beta) = N(\alpha)N(\beta)$ สำหรับทุกๆสมาชิก $\alpha , \beta \in D$

<u>ทฤษฎี 6.5.1</u> ถ้า D เป็นอินทิกรัลโดเมนบนซึ่งมี N เป็นนอร์มของการคูณบน D แล้วจะได้ว่า

1. $N(e) = 1$ เมื่อ e คือยูนิตี้ใน D และ 1 คือยูนิตี้ใน I
2. $N(u) = 1$ สำหรับทุกๆยูนิต u ใน D

<u>พิสูจน์</u> ให้ D เป็นอินติกรัลโดเมนมี N เป็นนอร์มของการคูณ

1. จากนิยาม 6.5.1 ข้อ 1, 3 จะได้ว่า

$N(e)\,1 = N(ee) = N(e)\,N(e) > 0$ เพราะ $e \neq 0$

ดังนั้น $1 = N(e)$

2. ให้ u เป็นยูนิตของ D ดังนั้นจะมี $u^{-1} \in D$ ซึ่ง

$uu^{-1} = e$

เพราะฉะนั้น $N(uu^{-1}) = N(e)$

นั่นคือ $N(u)N(u^{-1}) = 1$

เนื่องจาก $N(u), N(u^{-1})$ เป็นจำนวนเต็มที่ไม่เป็นลบ

ดังนั้นจะได้ว่า $N(u) = 1$ และ $N(u^{-1}) = 1$

แบบฝึกหัด 6 ข

1. จงพิสูจน์เล็มม่า 6.4.1 ข้อ 2, 3
2. จงหายูนิตทั้งหมดใน $I(i)$
3. ถ้า $a + bi$ ไม่ใช่ยูนิตของ $I(i)$ จงพิสูจน์ว่า $a^2 + b^2 > 1$
4. จงพิสูจน์ว่าไอดีลที่ไม่ใช่ศูนย์ (non - zero ideal) ในจำนวนเต็มเกาส์เซี่ยน $I(i)$ จะต้องมีจำนวนเต็ม
5. จงพิสูจน์ว่า ดิวิชันอัลกอริทึม ยังคงใช้ได้ใน $I(i)$ สำหรับ ν ซึ่งกำหนดโดย $\nu(\alpha) = N(\alpha)$ สำหรับ α ที่ไม่ใช่ศูนย์ของ $I(i)$

   (Hint : สำหรับ α และ β ใน $I(i)$ ซึ่ง $\beta \neq 0$, $\alpha/\beta = r + si$ ในเซ็ตของจำนวนเชิงซ้อน C และ r , $s \in Q$ ซึ่งเป็นเซ็ตของจำนวนตรรกยะ ให้ q_1 และ q_2 เป็น rational integer ใน I ที่มีค่าใกล้เคียงที่สุดกับจำนวนตรรกยะ r และ s ตามลำดับ จงแสดงให้เห็นว่า $\gamma = q_1 + q_2 i$ และ $\rho = \alpha - \beta\gamma$ ตัวหนึ่งมี $N(\rho) < N(\beta)$ โดยการแสดงว่า

   $$N(\rho) / N(\beta) = |(\alpha/\beta) - \gamma|^2 < 1$$

   ในที่นี้ $|\ |$ คือ ค่าสัมบูรณ์ (absolute value) ของสมาชิกใน C
6. ใช้ยูคลิเดียนอัลกอริทึมใน $I(i)$ หา gcd ของ $16 + 7i$ และ $10 - 5i$ ใน $I(i)$ [ใช้วิธีการในข้อ 5]