2 คณิตศาสตร์พื้นฐาน
Basic Mathematics

เพื่อให้ผู้อ่านมีความเข้าใจเนื้อหาของทฤษฎีรหัสได้ดีขึ้น และเพื่อความสมบูรณ์ของเนื้อหา ในที่นี้ เราจะทบทวนความรู้พื้นฐานทางคณิตศาสตร์ที่จำเป็นต่อการศึกษาทฤษฎีรหัส โดยจะละข้อพิสูจน์ของบางทฤษฎีบทไว้ ผู้อ่านที่สนใจสามารถหารายละเอียดเพิ่มเติมได้จากตำรามาตรฐานทางพีชคณิตนามธรรม หรือพีชคณิตเชิงเส้นทั่วไป

2.1 กรุป ริง ฟิลด์

กรุป ริง และฟิลด์ เป็นโครงสร้างทางคณิตศาสตร์ ที่ทำให้เราสามารถบวก ลบ คูณ และหาร สัญลักษณ์ที่ใช้ในการสร้างรหัสได้ เราเรียก การบวก ลบ คูณ และหาร ว่าการดำเนินการทวิภาค ส่วนใหญ่เราจะพูดถึงการบวกและการคูณ ส่วนการลบและการหารจะเป็นการดำเนินการผกผันของการบวกและการคูณตามลำดับ

นิยาม 2.1.1 การดำเนินการทวิภาค $\bullet$ บนเซต G คือฟังก์ชัน $\bullet : G \times G \rightarrow G$ สำหรับ $a, b \in G$ จะเขียนแทน $\bullet(a, b)$ ด้วย $a \bullet b$

กล่าวคือ การดำเนินการทวิภาคบนเซต G คือกฎเกณฑ์การกำหนดสมาชิก $a \bullet b$ ใน G ให้แก่คู่อันดับ (a, b) ใน GxG ในกรณีนี้ เรากล่าวว่า G มีสมบัติปิดภายใต้การดำเนินการ $\bullet$

กรุปเป็นโครงสร้างทางคณิตศาสตร์ที่สำคัญ ที่ประกอบด้วยเซตที่ไม่ใช่เซตว่าง และการดำเนินการทวิภาคหนึ่งอย่าง และสอดคล้องกับคุณสมบัติบางอย่าง

นิยาม 2.1.2

ถ้า G ไม่ใช่เซตว่าง เซต G จะเป็นกรุป ถ้ามีการดำเนินการทวิภาค • บน G ซึ่งสอดคล้องกับสมบัติต่อไปนี้

1. ถ้า $a, b \in G$ แล้ว $a \bullet b \in G$
   ในกรณีนี้เรากล่าวว่า G มีสมบัติปิดภายใต้การดำเนินการ •
2. ถ้า $a, b, c \in G$ แล้ว $a \bullet (b \bullet c) = (a \bullet b) \bullet c$
   ในกรณีนี้เรากล่าวว่ากฎการเปลี่ยนหมู่ใช้ได้ใน G
3. จะต้องมีสมาชิก e ใน G ซึ่ง $a \bullet e = e \bullet a = a$ สำหรับทุก ๆ $a \in G$
   ในกรณีนี้เราเรียก e ว่าเอกลักษณ์ของ G
4. แต่ละสมาชิก $a \in G$ ต้องมีสมาชิก $b \in G$ ซึ่ง $a \bullet b = b \bullet a = e$
   ในกรณีนี้ เรากล่าวว่า b เป็นตัวผกผันของ a และจะแทน b ด้วย a^{-1} ในกรณีที่การดำเนินการใน G เป็นการดำเนินการบวก เรานิยมแทน b ด้วย $-a$ และจะเรียก b ว่าเป็นลบ a

ถ้า G เป็นกรุปภายใต้การดำเนินการ • เราจะกล่าวว่า (G, •) เป็นกรุป หรือในกรณีที่ไม่ทำให้สับสน เราจะกล่าวว่า G เป็นกรุป โดยละการดำเนินการ • ไว้

นิยาม 2.1. 3

ถ้า $a \bullet b = b \bullet a$ สำหรับทุก ๆ $a, b \in G$ เราจะเรียก G ว่าอาบีเลียนกรุป หรือ กรุปสลับที่

หมายเหตุ :

1. ตัวผกผันของ e ก็คือ e เมื่อ e เป็นเอกลักษณ์ในกรุป G
2. เรียก $a \bullet b$ ว่าผลคูณของ a และ b
3. เพื่อความสะดวก เราจะเขียน ab แทน $a \bullet b$
4. แทน $a \bullet a \bullet \ldots \bullet a$ (n ตัว)ด้วย a^n ดังนั้น $a^n \bullet a^m = a^{n+m}$
5. แทน $(a^{-1})^n$ ด้วย a^{-n}

ตัวอย่าง 2.1.1 : เราเรียกกรุปที่มีจำนวนสมาชิกจำกัดว่า ***กรุปจำกัด*** มิฉะนั้นจะเรียกว่า ***กรุปไม่จำกัด*** ข้อ 1–5 ข้างล่างนี้เป็นตัวอย่างของกรุปไม่จำกัด

1. ให้ **Z** แทนเซตของจำนวนเต็ม จะเห็นว่า **Z** เป็นอาบีเลียนกรุปภายใต้การดำเนินการ + ตามปกติจะเห็นว่าจำนวนเต็ม 0 เป็นเอกลักษณ์ภายใต้การดำเนินการ + ถ้า a เป็นสมาชิกใน **Z** นั่นคือ a เป็นจำนวนเต็มใด ๆ ตัวผกผันของ a คือ –a เช่น ตัวผกผันของ 2 ภายใต้การบวกคือ –2 นอกจากนี้ เราสามารถตรวจสอบได้ไม่ยากนักว่า **Z** มีสมบัติปิดและสอดคล้องกับกฎการเปลี่ยนหมู่ ดังนั้น **Z** เป็นกรุปภายใต้การบวก ยิ่งไปกว่านั้นคือ **Z** เป็นอาบีเลียนกรุป

2. ให้ $\mathbf{Q} = \{\frac{a}{b} \mid a, b \in \mathbf{Z} \text{ เมื่อ } b \neq 0\}$ เป็นเซตของจำนวนตรรกยะ จะเห็นว่า (**Q**, +) เป็นอาบีเลียนกรุปภายใต้การ + ปกติเช่นกัน มี 0 เป็นเอกลักษณ์ ถ้า a เป็นจำนวนตรรกยะใด ๆ ตัวผกผันของ a ภายใต้การดำเนินการ + ก็คือ –a เช่น ตัวผกผันของ $\frac{1}{2}$ ก็คือ $-\frac{1}{2}$ และตัวผกผันของ –3 ก็คือ 3 เป็นต้น

3. ให้ **R** แทนเซตของจำนวนจริง จะเห็นว่า (**R**, +) เป็นอาบีเลียนกรุปภายใต้การ + ปกติ มี 0 เป็นเอกลักษณ์ ถ้า a เป็นจำนวนจริงใด ๆ ตัวผกผันของ a ภายใต้การดำเนินการ + ก็คือ –a

4. ให้ $\mathbf{Q}^*$ เป็นเซตของจำนวนตรรกยะทั้งหลายยกเว้น 0 กล่าวคือ $\mathbf{Q}^* = \mathbf{Q} - \{0\}$ เราสามารถตรวจสอบได้ไม่ยากนักว่า ($\mathbf{Q}^*$, x) เป็นอาบีเลียนกรุปภายใต้การคูณปกติ มี 1 เป็นเอกลักษณ์ภายใต้การคูณ สมาชิกแต่ละตัวใน $\mathbf{Q}^*$ มีตัวผกผัน เช่น ตัวผกผันของ $\frac{1}{2}$ ก็คือ 2 เพราะ $\frac{1}{2} \times 2 = 1$ และตัวผกผันของ 3 ก็คือ $\frac{1}{3}$ เพราะ $3 \times \frac{1}{3} = 1$ เป็นต้น

5. ให้ R^* เป็นเซตของจำนวนจริงทั้งหลายยกเว้น 0 กล่าวคือ $R^* = R - \{0\}$ เราสามารถตรวจสอบได้ไม่ยากนักว่า $(R^*, \times)$ เป็นอาบีเลียนกรุปภายใต้การคูณปกติ มี 1 เป็นเอกลักษณ์ภายใต้การคูณ และสมาชิกแต่ละตัวใน R^* มีตัวผกผัน

6. ทั้ง Z และ $Z^* = Z - \{0\}$ ไม่เป็นกรุปภายใต้การคูณปกติ เพราะขาดสมบัติข้อ 4 ของกรุป สมาชิกบางตัว เช่น 2 ไม่มีตัวผกผันในเพราะไม่สามารถหาสมาชิกใน Z หรือ Z^* ซึ่งเมื่อคูณกับ 2 แล้วเท่ากับ 1

ทฤษฎีบท 2.1.1

ถ้า G เป็นกรุป แล้ว

1. เอกลักษณ์ของ G จะมีตัวเดียวเท่านั้น (unique)
2. ตัวผกผันของสมาชิกแต่ละตัวใน G จะมีเพียงตัวเดียวเท่านั้น
3. $(a^{-1})^{-1} = a$ สำหรับ a ใด ๆ ใน G
4. $(ab)^{-1} = b^{-1}a^{-1}$ สำหรับ a, b ใด ๆ ใน G

กรุปในตัวอย่าง 2.1.1 ล้วนเป็นกรุปไม่จำกัด ต่อไปจะแนะนำให้รู้จักกรุปจำกัดที่สำคัญที่จะพบเห็นเสมอๆ ในวิชาทฤษฎีรหัส นั่นก็คือกรุปของจำนวนเต็มมอดุโล n

เซตของจำนวนเต็มมอดุโล n

เป็นเซตซึ่งมีบทบาทสำคัญมากในวิชาทฤษฎีรหัสเชิงพีชคณิต มีโครงสร้างทางคณิตศาสตร์ที่ทำให้เราสามารถบวก ลบ คูณ และหารสมาชิกในเซตได้

นิยาม 2.1.4

ให้ n เป็นจำนวนเต็มบวก $a, b \in Z$ เรากล่าวว่า a สมภาค (congruence) กับ b มอดุโล n ถ้า n หาร $a - b$ ลงตัว หรือ $a = kn + b$ สำหรับ k ที่เป็นจำนวนเต็มบางจำนวน และจะเขียน $a \equiv b \pmod{n}$

ตัวอย่าง 2.1.2 :

1. $7 \equiv 2 \pmod 5$ เพราะ $5 \mid (7 - 2)$
2. $13 \equiv 1 \pmod 2$ เพราะ $2 \mid (13 - 1)$
3. $-10 \equiv 2 \pmod 3$ เพราะ $3 \mid (-10 - 2)$
4. $103 \not\equiv 3 \pmod 7$ เพราะว่า $7 \nmid (103 - 3)$

ถ้าให้ $Z_n = \{0, 1, \ldots, n-1\}$ และ a เป็นจำนวนเต็มใด ๆ จะเห็นว่าเมื่อหาร a ด้วย n จะเหลือเศษเป็นจำนวนใดจำนวนหนึ่งใน $Z_n = \{0, 1, \ldots, n-1\}$ เพียงจำนวนเดียวเท่านั้น กล่าวอีกนัยหนึ่งคือสมการ $x \equiv a \pmod n$ มีผลเฉลยใน Z_n และมีเพียงผลเฉลยเดียวเท่านั้น เช่น ใน $Z_5 = \{0, 1, 2, 3, 4\}$ ผลเฉลยของสมการ $x \equiv 36 \pmod 5$ คือ $x = 1$ เพราะ 1 เป็นเศษที่เหลือจากการหาร 36 ด้วย 5

ให้ $a, b \in Z_n$ เรานิยามการบวกและการคูณใน Z_n ดังนี้

การบวกมอดุโล n

$a +_n b$ = เศษที่เหลือจากการหารผลบวก $a + b$ ด้วย n

การคูณมอดุโล n

$a \times_n b$ = เศษที่เหลือจากการหารผลคูณ ab ด้วย n

ตัวอย่าง 2.1.3 :

1. ใน Z_3

   $4 +_3 5 = 0$ เพราะ $4 + 5 = 9$ เมื่อหาร 9 ด้วย 3 แล้วเหลือเศษ 0

   $4 \times_3 5 = 2$ เพราะ $4 \times 5 = 20$ เมื่อหาร 20 ด้วย 3 เหลือเศษ 2

2. ใน Z_5

   $9 +_5 8 = 2$ เพราะ $9 + 8 = 17$ เมื่อหาร 17 ด้วย 5 เหลือเศษ 2

   $9 \times_5 8 = 2$ เพราะ $9 \times 8 = 72$ เมื่อหาร 72 ด้วย 5 เหลือเศษ 2

   ในกรณีที่ไม่ทำให้สับสน เราจะเขียน + และ $\times$ แทน $+_n$ และ $\times_n$

ตามลำดับ นอกจากนี้ เราจะเขียน ab แทน a x_n b และสำหรับกรณีที่ไม่ทำให้เข้าใจสับสน เราจะเรียกการบวกมอดุโล n และการคูณมอดุโล n ง่าย ๆ ว่าการบวกและการคูณ ตามลำดับ

ตัวอย่าง 2.1.4 : ใน $Z_2 = \{0, 1\}$ เราแสดงการบวกและการคูณใน Z_2 ด้วยตารางข้างล่างนี้

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

ตัวอย่าง 2.1.5 : ใน $Z_3 = \{0, 1, 2\}$ เราแสดงการบวกและการคูณในตารางต่อไปนี้

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

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

ตัวอย่าง 2.1.6 : ใน $Z_5 = \{0, 1, 2, 3, 4, 5\}$ } เราแสดงการบวกและการคูณในตารางต่อไปนี้

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

จะเห็นว่า

1. $(Z_5, +)$ เป็นอาบีเลียนกรุปภายใต้การบวกมอดุโล 2
   มี 0 เป็นเอกลักษณ์ สมาชิกแต่ละตัวใน Z_5 มีตัวผกผัน ตัวผกผันของ 0 คือ 0 และตัวผกผันของ 1 คือ 1 นั่นคือ – 0 = 0 และ

$-1 = 1$ ทั้งนี้เพราะว่า $0 + 0 = 0$ และ $1 + 1 = 0$ มอดุโล 2

2. $(Z_3,+)$ เป็นอาบีเลียนกรุปภายใต้การบวกมอดุโล 3
   มี 0 เป็นเอกลักษณ์ สมาชิกแต่ละตัวใน Z_3 มีตัวผกผัน
   $$-0 = 0, -1 = 2, \text{ และ } -2 = 1$$
3. $(Z_5,+)$ เป็นอาบีเลียนกรุปภายใต้การบวกมอดุโล 5
   มี 0 เป็นเอกลักษณ์ และ
   $$-1 = 4, \ -2 = 3, \ -3 = 2 \text{ และ } -4 = 1$$
4. ในกรณีทั่วไป $(Z_n,+)$ เป็นอาบีเลียนกรุปภายใต้การบวกมอดุโล n
5. (Z_n, x) ไม่เป็นกรุปภายใต้การบวกมอดุโล n เพราะ 0 ไม่มีตัวผกผัน

นิยาม 2.1.5 ถ้า H เป็นเซตย่อยที่ไม่ใช่เซตว่างของกรุป G จะเรียก H ว่า กรุปย่อย ของ G ถ้า H เป็นกรุปภายใต้การดำเนินการใน G

ตัวอย่าง 2.1.7 : พิจารณากรุป (Z, +) ถ้าให้ E เป็นเซตของจำนวนเต็มคู่ทั้งหลายของ Z นั่นคือ

$$E = \{ \ldots, -6, -4, -2, 0, 2, 4, 6 \ldots \}$$

เราสามารถตรวจสอบได้ไม่ยากนักว่า E มีสมบัติทั้ง 4 ข้อ ของกรุป นั่นคือ E เป็นกรุปภายใต้การบวก ดังนั้น E เป็นกรุปย่อยของ Z

ตัวอย่าง 2.1.8 : พิจารณากรุป (Z, +) ถ้าให้ n เป็นจำนวนเต็มใด ๆ และ

$$nZ = \{nz \mid z \in Z\}$$

นั่นคือ nZ เป็นเซตของพหุคูณของ n เช่นเดียวกับตัวอย่าง 2.1.7 เราสามารถตรวจสอบได้ไม่ยากนักว่า nZ เป็นกรุปย่อยของ Z

หมายเหตุ : จะเห็นว่าเซต E ในตัวอย่าง 2.1.7 ก็คือ เซตของพหุคูณของ 2 หรือ 2Z นั่นเอง

ทฤษฎีบท 2.1.2

ถ้า $(G, \bullet)$ เป็นกรุปและ H เป็นเซตย่อยของ G ที่ไม่ใช่เซตว่าง H จะเป็นกรุปย่อยของ G ก็ต่อเมื่อสมบัติทั้งสองข้อต่อไปนี้เป็นจริง

1. ถ้า $a, b \in H$ แล้ว $a \bullet b \in H$ นั่นคือ H มีสมบัติปิดภายใต้การดำเนินการ $\bullet$
2. ถ้า $a \in H$ แล้ว $a^{-1} \in H$

ตัวอย่าง 2.1.9 : พิจารณา $Z_6 = \{0, 1, 2, 3, 4, 5\}$ ซึ่งเป็นกรุปภายใต้การบวกมอดุโล 6 ให้

$$H = \{0, 2, 4\}$$

เป็นเซตย่อยของ Z_6 จะเห็นว่า H มีสมบัติปิดภายใต้การดำเนินการบวกมอดุโล 6 และเนื่องจาก $2 + 4 \equiv 0 \pmod 6$ หรือเขียน $2 +_6 4 = 0$ หรือเขียน $2 + 4 = 0$ ถ้าไม่ทำให้เข้าใจสับสน ดังนั้น ตัวผกผันของ 2 คือ 4 ในทางกลับกันตัวผกผันของ 4 คือ 2 หรือเขียน $-2 = 4$ และ $-4 = 2$ ตามลำดับ นั่นคือสมาชิกทุกตัวใน H มีตัวผกผัน ดังนั้น H เป็นกรุปย่อยของ Z_6 ซึ่งมี 0 เป็นเอกลักษณ์ของ H เช่นกัน

นิยาม 2.1.6

ให้ H เป็นกรุปย่อยของ G และ $a \in G$ จะเรียก

$$aH = \{ah \mid \text{สำหรับทุก } h \in H\}$$

ว่าโคเซตซ้ายของ H ใน G และเรียก

$$Ha = \{ha \mid \text{สำหรับทุก } h \in H\}$$

ว่าโคเซตขวาของ H ใน G

หมายเหตุ :

1. ในกรณีที่การดำเนินการใน G เป็นการดำเนินการบวก หรือในกรณีที่ G เป็นอาบีเลียนกรุป เรานิยมเขียน $a + H$ และ $H + a$ แทน aH และ Ha ตามลำดับ

2. ถ้า G เป็นอาบีเลียนกรุปแล้วโคเซตซ้ายจะเท่ากับโคเซตขวาเสมอ นั่นคือ a + H = H + a สำหรับ a ใด ๆ ใน G เนื่องจากเราจะสนใจเฉพาะอาบีเลียนกรุปเท่านั้น ดังนั้น เราจะเรียกโคเซตโดยไม่ต้องระบุว่าเป็นโคเซตซ้ายหรือโคเซตขวา

ตัวอย่าง 2.1.10 : จากตัวอย่าง 2.1.9 เรามี $Z_6 = \{0, 1, 2, 3, 4, 5\}$ เป็นอาบีเลียนกรุปภายใต้การบวก และมี $H = \{0, 2, 4\}$ เป็นกรุปย่อยของ Z_6 เราได้

$0 + H = \{0, 2, 4\} = H$

$1 + H = \{1, 3, 5\}$

$2 + H = \{2, 4, 0\} = 0 + H$

$3 + H = \{3, 5, 1\} = 1 + H$

$4 + H = \{4, 0, 2\} = 0 + H$

$5 + H = \{5, 1, 3\} = 1 + H$

แสดงว่าโคเซตของ H ใน Z_6 มีเพียง 2 โคเซตเท่านั้นที่แตกต่างกัน คือ H และ 1 + H

ข้อสังเกต : จากตัวอย่าง 2.1.10 ข้างบนนี้ เห็นได้ชัดว่า

1. แต่ละโคเซตมีจำนวนสมาชิกเท่ากัน
2. สองโคเซตใด ๆ จะไม่มีสมาชิกร่วมกัน เช่น 0 + H และ 1 + H หรือมิฉะนั้นก็เท่ากัน เช่น 1 + H และ 3 + H
3. ยูเนียนของโคเซตทั้งหลายจะเท่ากับ Z_6

ในกรณีทั่วไป เราได้ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.1.3

ถ้า G เป็นกรุปและ H เป็นกรุปย่อยของ G แล้ว

1. $a \in bH$ ก็ต่อเมื่อ $aH = bH$
2. $aH = bH$ ก็ต่อเมื่อ $b^{-1}a \in H$
3. $aH \cap bH = \phi$ หรือมิฉะนั้น $aH = bH$

4. $\bigcup_{a \in G} aH = G$

5. $|aH| = |H|$ เมื่อ G เป็นกรุปจำกัด และ $a \in G$

พิสูจน์ (1) สมมุติให้ $a \in bH$ ดังนั้น

$$a = bh \text{ หรือ } b = ah^{-1}$$

สำหรับบาง $h \in H$ เราจะแสดงว่า $aH = bH$

สมมุติให้ x เป็นสมาชิกใด ๆ ใน aH เราได้ $x = ah_1$ สำหรับ h_1 ที่เป็นสมาชิกบางตัวของ H ดังนั้น

$$x = ah_1 = (bh)h_1 = b(hh_1)$$

เนื่องจาก h และ h_1 เป็นสมาชิกของ H และ H เป็นกรุป จากสมบัติของกรุป แสดงว่าผลคูณ hh_1 ต้องเป็นสมาชิกใน H นั่นคือ $x \in bH$ เราได้ $aH \subset bH$

ในทำนองเดียวกัน สมมุติให้ x เป็นสมาชิกใด ๆ ใน bH เราได้ $x = bh_2$ สำหรับ h_2 ที่เป็นสมาชิกบางตัวของ H ดังนั้น

$$x = bh_2 = (ah^{-1})h_2 = a(h^{-1}h_2)$$

แสดงว่า $x \in aH$ ดังนั้น $bH \subset aH$ เราสรุปได้ว่า $aH = bH$ ตามต้องการ

พิสูจน์ (2) สมมุติให้ $aH = bH$ จะแสดงว่า $b^{-1}a \in H$

เนื่องจาก $a \in aH$ ดังนั้น $a \in bH$ แสดงว่าจะต้องมี $h \in H$ ซึ่ง $a = bh$ ดังนั้น $b^{-1}a = h \in H$

ในทางกลับกัน สมมุติให้ $b^{-1}a \in H$ ดังนั้น $b^{-1}a = h$ สำหรับบาง $h \in H$ ซึ่งเป็นผลให้ $a = bh \in bH$ และจากข้อ 1 เราได้

$$aH = bH$$

ตามต้องการ

พิสูจน์ (3) ให้ aH และ bH เป็นโคเซตสองโคเซตใด ๆ ใน G เราจะแสดงว่า

$$aH \cap bH = \phi \text{ หรือมิฉะนั้น } aH = bH$$

สมมุติว่า $aH \cap bH \neq \phi$ ดังนั้นจะต้องมี $x \in aH \cap bH$ แสดงว่า $x \in aH$ และ $x \in bH$ นั่นคือ $x = ah_1$ และ $x = bh_2$ สำหรับบาง $h_1, h_2 \in H$ เราได้

$$x = ah_1 = bh_2 \text{ ซึ่งเป็นผลให้ } a = bh_2h_1^{-1} = bh_3$$

เมื่อ $h_3 = h_2h_1^{-1}$ แสดงว่า $a \in bH$ ดังนั้น จากข้อ 1 เราได้

$$aH = bH$$

พิสูจน์ (4) ให้ $x \in \bigcup_{a \in G} aH$ แสดงว่า x เป็นสมาชิกของบางโคเซต สมมุติว่า $x \in aH$ สำหรับบางสมาชิก a ใน G แสดงว่า x ต้องเป็นสมาชิกใน G เราได้ $\bigcup_{a \in G} aH \subset G$

ในทางกลับกัน สมมุติให้ $x \in G$ ดังนั้น $x \in xH$ ซึ่งเป็นผลให้ $x \in \bigcup_{a \in G} aH$ นั่นคือ $G \subset \bigcup_{a \in G} aH$ จาก

$$\bigcup_{a \in G} aH \subset G \text{ และ } G \subset \bigcup_{a \in G} aH$$

สรุปได้ว่า $\bigcup_{a \in G} aH = G$ ตามต้องการ

พิสูจน์ (5) เนื่องจาก G เป็นกรุปจำกัด เราให้ $H = \{h_1, h_2, \ldots, h_n\}$ เป็นกรุปย่อยของ G ให้ a เป็นสมาชิกใด ๆ ใน G เราได้

$$aH = \{ah_1, ah_2, \ldots, ah_n\}$$

เราจะแสดงว่าสมาชิกของ aH แตกต่างกันทั้งหมด โดยสมมุติว่า $ah_i = ah_j$ สำหรับ i และ j ที่แตกต่างกัน เราได้ $h_i = h_j$ ซึ่งเป็นไปไม่ได้ แสดงว่าจำนวนสมาชิกใน aH เท่ากับจำนวนสมาชิกใน H ■

ถ้าให้ |X| แทนขนาดของเซต X และกรุปจำกัดหมายถึงกรุปที่มีจำนวนสมาชิกจำกัด เราได้ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.1.4

Lagrange's Theorem

ถ้า G เป็นกรุปจำกัดและ H เป็นกรุปย่อยของ G แล้ว |H| หาร |G| ได้ลงตัว

หมายเหตุ : บทกลับของ Lagrange's Theorem ไม่เป็นจริง นั่นคือถ้า k หาร |G| ได้ลงตัวแล้ว ไม่จำเป็นเสมอว่า G จะต้องมีกรุปย่อยที่มีขนาด k

นิยาม 2.1.7

กรุปย่อย H ของ G เป็นกรุปย่อยปกติของ G ถ้า aH = Ha สำหรับทุก $a \in G$

หมายเหตุ : กรุปย่อยของอาบีเลียนกรุปเป็นกรุปย่อยปกติ

ทฤษฎีบท 2.1.5

ให้ H เป็นกรุปย่อยปกติของ G ถ้าให้ G/H แทนเซตของโคเซตทั้งหลายของ H ใน G แล้ว G/H จะเป็นกรุปภายใต้การดำเนินการ (aH)(bH) = abH

นิยาม 2.1.8

ให้ H เป็นกรุปย่อยปกติของ G จะเรียกกรุป G/H ว่ากรุปผลหารของ G มอดุโล H และจะอ่าน G/H ว่า G มอด H

ตัวอย่าง 2.1.11 : จากตัวอย่าง 2.1.10 เราได้

$$G/H = \{ H, 1 + H\}$$

เป็นกรุปที่มี H หรือ 0 + H เป็นเอกลักษณ์ ตัวผกผันของ 1 + H คือ 5 + H เพราะว่า

$$(1 + H) + (5 + H) = (1 + 5) + H = 0 + H = H$$

แต่ในตัวอย่าง 2.1.10 เช่นกัน เรารู้ว่า $5 + H = 1 + H$ ดังนั้น เราอาจกล่าวว่า ตัวผกผันของ $1 + H$ ก็คือ $1 + H$ เอง

นิยาม 2.1.9 ให้ R เป็นเซตที่ไม่ใช่เซตว่าง R จะเป็นริง ถ้ามีการดำเนินการบวก + และคูณ • ซึ่งสอดคล้องกับสมบัติต่อไปนี้

1. ถ้า $a, b \in R$ แล้ว $a + b \in R$
2. $(a + b) + c = a + (b + c)$ สำหรับ a, b, c ที่เป็นสมาชิกใด ๆ ใน R
3. มีสมาชิก $0 \in R$ ซึ่ง $a + 0 = 0 + a = a$ สำหรับ a ใด ๆ ใน R
4. ถ้า $a \in R$ จะต้องมี $b \in R$ ซึ่ง $a + b = b + a = 0$ ในกรณีนี้เราแทน b ด้วย $-a$
5. $a + b = b + a$ สำหรับ a, b ใด ๆ ใน R
6. ถ้า $a, b \in R$ แล้ว $a \bullet b \in R$
7. $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ สำหรับ a, b, c ที่เป็นสมาชิกใด ๆ ใน R
8. สำหรับ a, b, c ที่เป็นสมาชิกใด ๆ ใน R

$$a \bullet (b + c) = a \bullet b + a \bullet c$$

และ $$(b + c) \bullet a = b \bullet a + c \bullet a$$

หมายเหตุ :

1. จากสมบัติข้อ 1 – 4 แสดงว่า R เป็นกรุปภายใต้การบวก
2. จากสมบัติข้อ 1 – 5 แสดงว่า R เป็นอาบีเลียนกรุปภายใต้การบวก
3. เรียกสมบัติข้อ 8 ว่า สมบัติการแจกแจง
4. เพื่อความสะดวก บางครั้งเราเขียน ab แทน $a \bullet b$

ตัวอย่าง 2.1.12 :

1. **Z, Q, R** เป็นริงภายใต้การดำเนินการบวกและการคูณปกติ ริงทั้งสามมี 0 เป็นเอกลักษณ์
2. $\mathbf{Z}_n$ เป็นริงภายใต้การบวกและการคูณมอดุโล n มี 0 เป็นเอกลักษณ์

นิยาม 2.1.10

ถ้าในริง R มีสมาชิก 1 ซึ่ง $1 \cdot a = a \cdot 1 = a$ สำหรับ a ใด ๆ ใน R เราจะเรียก R ว่า ริงที่มี 1 และถ้า $a \cdot b = b \cdot a$ สำหรับ a, b ใด ๆ ใน R เราจะเรียก R ว่า ริงสลับที่

ตัวอย่าง 2.1.13 :

1. **Z, Q, R** และ $\mathbf{Z}_n$ ในตัวอย่าง 2.1.12 เป็นริงสลับที่ที่มี 1 ซึ่งเป็นเอกลักษณ์ภายใต้การคูณ
2. เซต E ของจำนวนเต็มคู่ เป็นริงสลับที่ภายใต้การบวกและการคูณปกติ แต่ไม่มีเอกลักษณ์การคูณ คือไม่มี 1

ทฤษฎีบท 2.1.6

ถ้า R เป็นริงและ $a, b \in R$ แล้ว

1. $a(-b) = (-a)b = -(ab)$
2. $(-a)(-b) = ab$

และถ้า R เป็นริงที่มี 1 แล้ว

3. $(-1)a = -a$
4. $(-1)(-1) = 1$

นิยาม 2.1.11

ให้ R เป็นริง จะเรียกเซตย่อย I ของ R ที่ไม่ใช่เซตว่างว่า ไอดีล ของริง R ถ้า

1. I เป็นกรุปย่อยของ R ภายใต้การบวก
2. $ra \in I$ สำหรับทุก ๆ $r \in R$ และ $a \in I$

ตัวอย่าง 2.1.14 : จากตัวอย่าง 2.1.8 เรารู้ว่า

$$2\mathbf{Z} = \{ \ldots, -6, -4, -2, 0, 2, 4, 6, \ldots \}$$

เป็นกรุปย่อยของ **Z** ภายใต้การบวก และสำหรับ k ที่เป็นจำนวนเต็มใด ๆ ใน **Z** จะพบว่า $ka \in 2\mathbf{Z}$ สำหรับทุก ๆ $a \in 2\mathbf{Z}$ ดังนั้น $2\mathbf{Z}$ เป็นไอดีลของ **Z**

หมายเหตุ : ไอดีล I ของริง R เป็นกรุปย่อยปรกติของ R ภายใต้การบวก ดังนั้น

$$R / I = \{a + I \mid a \in R\}$$

เป็นกรุปผลหาร อ่านว่า R มอดุโล I หรือ R มอด I

นิยาม 2.1.12 ถ้า F เป็นริงสลับที่ที่มี 1 จะเรียก F ว่าฟิลด์ ถ้ามีสมาชิก $b \in F$ ซึ่ง $ab = 1$ สำหรับสมาชิก a ใด ๆ ใน F ที่ไม่ใช่ 0

จากนิยาม 2.1.12 จะเห็นว่า F เป็นฟิลด์ก็ต่อเมื่อ

1. F เป็นกรุปสลับที่ภายใต้การบวก
2. $F^* = F - \{0\}$ เป็นกรุปสลับที่ภายใต้การคูณ
3. F สอดคล้องกับสมบัติการแจกแจง

ตัวอย่าง 2.1.15 :

1. **Q** และ **R** เป็นฟิลด์
2. **Z** เป็นริงแต่ไม่เป็นฟิลด์ เพราะสมาชิกที่ไม่ใช่ 0 บางตัวใน **Z** ไม่มีตัวผกผันภายใต้การคูณ เช่น 2 ไม่มีตัวผกผัน ดังนั้น $\mathbf{Z}^*$ จึงไม่เป็นกรุปภายใต้การคูณ
3. เราสามารถตรวจสอบได้ไม่ยากนักว่า $\mathbf{Z}_2$, $\mathbf{Z}_3$ และ $\mathbf{Z}_5$ เป็นฟิลด์ พิจารณา $\mathbf{Z}_5$ จะเห็นว่าสมาชิกแต่ละตัวใน Z_5 ที่ไม่ใช่ 0 มีตัวผกผันภายใต้การคูณ นั่นคือ

   $1^{-1} = 1, \quad 2^{-1} = 3, \quad 3^{-1} = 2 \quad$ และ $\quad 4^{-1} = 4$

4. $Z_6 = \{0, 1, 2, 3, 4, 5\}$ เป็นริงแต่ไม่เป็นฟิลด์ ภายใต้การบวกและการคูณมอดุโล 6 ทั้งนี้เพราะว่าสมาชิกที่ไม่ใช่ 0 บางตัวไม่มีตัวผกผันภายใต้การคูณ กล่าวคือ 2, 3 และ 4 ไม่มีตัวผกผัน

ทฤษฎีบท 2.1.7

> ถ้า F เป็นฟิลด์ แล้ว
>
> 1. $a0 = 0$ สำหรับทุก ๆ $a \in F$
> 2. ถ้า $ab = 0$ แล้ว $a = 0$ หรือ $b = 0$
>
> (ในกรณีนี้เรากล่าวว่า F ไม่มีตัวหารของ 0)

พิสูจน์(1) เรามี $a0 = a(0 + 0) = a0 + a0$ ดังนั้น

$$a0 - a0 = (a0 + a0) - a0 = a0 + (a0 - a0) = a0 + 0 = a0$$

นั่นคือ $0 = a0$

พิสูจน์ (2) สมมุติให้ $ab = 0$ และ $a \neq 0$ เราจะแสดงว่า $b = 0$ เนื่องจาก F เป็นฟิลด์ สมาชิกของ F ที่ไม่ใช่ 0 ต้องมีตัวผกผัน แสดงว่าต้องมี $a^{-1} \in F$ ซึ่ง $aa^{-1} = 1$ คูณสมการ $ab = 0$ ด้วย a^{-1} ทั้งสองข้าง เราได้

$$a^{-1}(ab) = a^{-1}0 = 0$$

ดังนั้น

$$(a^{-1}a)b = b = 0$$

ตามต้องการ ■

ทฤษฎีบท 2.1.8

> Z_p เป็นฟิลด์ก็ต่อเมื่อ p เป็นจำนวนเฉพาะ

พิสูจน์ ขั้นแรก สมมุติว่า Z_p เป็นฟิลด์ จะพิสูจน์ว่า p เป็นจำนวนเฉพาะ เราจะพิสูจน์โดยวิธีหาข้อขัดแย้ง ดังนั้น สมมุติว่า p ไม่ใช่จำนวนเฉพาะ นั่นคือ p เป็นจำนวนประกอบ สมมุติว่า $p = ab$ สำหรับ a, b ที่เป็นจำนวนเต็มบวกที่ทั้งคู่น้อยกว่า p ดังนั้น

$$a \not\equiv 0 \pmod{p} \text{ และ } b \not\equiv 0 \pmod{p}$$

นั่นคือ $a \neq 0$ และ $b \neq 0$ ใน Z_p ซึ่งเป็นไปไม่ได้ เพราะ Z_p เป็นฟิลด์ และ $ab = 0$ ใน Z_p แสดงว่า p ต้องเป็นจำนวนเฉพาะ

ในทางกลับกัน สมมุติให้ p เป็นจำนวนเฉพาะ เราจะแสดงว่า Z_p เป็นฟิลด์ เราทราบแล้วว่า Z_p เป็นริงสลับที่ที่มี 1 ดังนั้น ในการแสดงว่า Z_p เป็นฟิลด์ เราเพียงแสดงว่าสมาชิกแต่ละตัวที่ไม่ใช่ 0 มีตัวผกผันภายใต้การคูณใน Z_p

สมมุติให้ $a \neq 0 \in Z_p$ พิจารณาสมาชิก $p - 1$ ตัว ซึ่งเป็นผลคูณของ a กับสมาชิกของ Z_p ต่อไปนี้

$$1a, 2a, 3a, \ldots, (p-1)a$$

จะเห็นว่าไม่มีจำนวนใดหารด้วย p ได้ลงตัว นั่นคือ ไม่มีจำนวนใดสมภาคกับ 0 (mod p) และไม่มีจำนวนใดสมภาคกัน เพราะถ้า $ia \equiv ja \pmod p$ แล้ว $(i - j)a \equiv 0 \pmod p$ แสดงว่า $p \mid (i - j)a$ ดังนั้น $p \mid (i - j)$ เพราะว่า $p \nmid a$ ดังนั้น $i \equiv j \pmod p$ ซึ่งเป็นไปไม่ได้ แสดงว่า $1a, 2a, 3a, \ldots, (p-1)a$ ต้องเท่ากับ $1, 2, \ldots, p-1$ ดังนั้น ต้องมี $ja = 1$ สำหรับบาง j ที่เป็นจำนวนเต็มบวกใน

$$Z_p = \{0, 1, 2, \ldots, p-1\}$$

นั่นคือ j เป็นตัวผกผันของ a หรือ $j = a^{-1}$ นั่นเอง ■

ตัวอย่าง 2.1.16 : Z_7 เป็นฟิลด์ สมาชิกที่ไม่ใช่ 0 แต่ละตัวมีตัวผกผันภายใต้การคูณ

$1 \times 1 = 1$ ดังนั้น $1^{-1} = 1$

$2 \times 4 = 1$ ดังนั้น $2^{-1} = 4$ และ $4^{-1} = 2$

$3 \times 5 = 1$ ดังนั้น $3^{-1} = 5$ และ $5^{-1} = 3$

$6 \times 6 = 1$ ดังนั้น $6^{-1} = 6$

2.2 ปริภูมิเวกเตอร์ (Vector Spaces)

รหัสที่เราจะศึกษาในที่นี้ ล้วนเป็นรหัสเชิงเส้นบนฟิลด์ F_q และรหัสเชิงเส้นก็คือปริภูมิย่อยของปริภูมิเวกเตอร์ F_q^n ดังนั้น ในหัวข้อนี้ เราจะ

ทบทวนความรู้เรื่องปริภูมิเวกเตอร์ โดยจะละการพิสูจน์ของทฤษฎีบทบางบทไว้ให้เป็นแบบฝึกหัดสำหรับผู้อ่าน

นิยาม 2.2.1 ให้ V เป็นเซตที่ไม่ใช่เซตว่าง มีสมาชิกซึ่งเรียกว่า *เวกเตอร์* ให้ F เป็นฟิลด์ มีสมาชิกซึ่งเรียกว่า *สเกลาร์* จะเรียก V ว่า *ปริภูมิเวกเตอร์* บนฟิลด์ F ถ้ามีการดำเนินการบวกและการคูณด้วยสเกลาร์ ซึ่งสอดคล้องกับสมบัติต่อไปนี้

สมบัติเกี่ยวกับการบวกเวกเตอร์

1. สมบัติปิด : ถ้า $x, y \in V$ แล้ว $x + y \in V$
2. สมบัติการเปลี่ยนหมู่ :
   ถ้า $x, y, z \in V$ แล้ว $x + (y + z) = (x + y) + z$
3. เอกลักษณ์ :มีสมาชิก 0 ใน V ซึ่ง $x + 0 = 0 + x = x$
   สำหรับทุก ๆ $x \in V$ (เรียก 0 ว่า *เวกเตอร์ศูนย์*)
4. ตัวผกผัน : ถ้า $x \in V$ แล้วจะมี $-x \in V$ ซึ่ง
   $x + (-x) = -x + x = 0$
5. สมบัติสลับที่ : ถ้า $x, y \in V$ แล้ว $x + y = y + x$

สมบัติเกี่ยวกับการคูณเวกเตอร์ด้วยสเกลาร์

6. สมบัติปิด : ถ้า $x \in V$ และ $c \in F$ แล้ว $cx \in V$
7. สมบัติการเปลี่ยนหมู่ : ถ้า $x \in V$ และ $b, c \in F$ แล้ว
   $(bc)x = b(cx)$
8. เอกลักษณ์ : ถ้า $x \in V$ แล้ว $1x = x$ เมื่อ 1 เป็นเอกลักษณ์ภายใต้การคูณใน F

สมบัติที่เชื่อมการบวกและการคูณเวกเตอร์ด้วยสเกลาร์

9. สมบัติการแจกแจง : ถ้า $x, y \in V$ และ $b, c \in F$ แล้ว
   $(b + c)x = bx + cx$
   และ $c(x + y) = cx + cy$

หมายเหตุ :

1. จากสมบัติข้อ 1 แสดงว่าผลบวกของเวกเตอร์เป็นเวกเตอร์
2. จากสมบัติข้อ 6 แสดงว่าการคูณเวกเตอร์ด้วยสเกลาร์ ผลลัพธ์จะเป็นเวกเตอร์
3. จากสมบัติข้อ 1 – 5 แสดงว่า V เป็นอาบีเลียนกรุปภายใต้การบวก

ตัวอย่าง 2.2.1 : ให้ R เป็นฟิลด์ของจำนวนจริง ให้ R^n แทนเซตของ n สิ่งอันดับของสมาชิกใน R นั่นคือ

$$R^n = \{ (x_1, x_2, \ldots, x_n) \mid x_i \in R \text{ สำหรับ } i = 1, 2, \ldots, n\}$$

ให้ $c \in R$ และ $\mathbf{x}, \mathbf{y} \in R^n$

$$\mathbf{x} = (x_1, x_2, \ldots, x_n), \quad \mathbf{y} = (y_1, y_2, \ldots, y_n)$$

ให้นิยามการบวกและการคูณด้วยสเกลาร์ ดังนี้

การบวก : $\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$

การคูณด้วยสเกลาร์ : $c\mathbf{x} = (cx_1, cx_2, \ldots, cx_n)$

เราสามารถตรวจสอบได้ไม่ยากนักว่า R^n สอดคล้องกับสมบัติทั้ง 9 ข้อของปริภูมิเวกเตอร์ภายใต้การบวกและการคูณด้วยสเกลาร์ ดังนั้น R^n เป็นปริภูมิเวกเตอร์บนฟิลด์ R จะเห็นว่า

1. $\mathbf{0} = (0, 0, \ldots, 0)$ เป็นเวกเตอร์ศูนย์ใน R^n และ
2. $-\mathbf{x} = (-x_1, -x_2, \ldots, -x_n)$

ตัวอย่าง 2.2.2 : ให้ P_2 เป็นเซตของพหุนามดีกรีน้อยกว่าหรือเท่ากับ 2 ที่มีสัมประสิทธิ์เป็นจำนวนจริง ให้

$$p = a_0 + a_1x + a_2x^2 \quad \text{และ} \quad q = b_0 + b_1x + b_2x^2$$

เป็นพหุนามใน P_2 และ c เป็นจำนวนจริงใด ๆ นิยามการดำเนินการดังนี้

การบวก : $p + q = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2$

การคูณด้วยสเกลาร์ : $cp = ca_0 + (ca_1)x + (ca_2)x^2$

P_2 เป็นปริภูมิเวกเตอร์ มีพหุนาม 0 เป็นเวกเตอร์ศูนย์ และ

$$-p = -a_0 - a_1x - a_2x^2$$

ตัวอย่าง 2.2.3 : ให้ M_{mxn}แทนเซตของเมทริกซ์ขนาด mxn ซึ่งมีสมาชิกเป็นจำนวนจริง เราสามารถตรวจสอบได้ไม่ยากนักว่า M_{mxn}เป็นปริภูมิเวกเตอร์ภายใต้การดำเนินการบวกและการคูณเมทริกซ์ด้วยสเกลาร์

ตัวอย่าง 2.2.4 : ให้ $F_q^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in F_q$ สำหรับ $i = 1, 2, \ldots, n\}$ เมื่อ F_q คือฟิลด์ที่มีขนาด q ให้

$$\mathbf{x} = (x_1, x_2, \ldots, x_n),\ \mathbf{y} = (y_1, y_2, \ldots, y_n) \in F_q^n \text{ และ } c \in F_q$$

เรานิยามการบวกและการคูณด้วยสเกลาร์ ในทำนองเดียวกับตัวอย่าง 2.2.1 นั่นคือ

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \text{ และ}$$

$$c\mathbf{x} = (cx_1, cx_2, \ldots, cx_n)$$

เมื่อ $x_i + y_i$ และ cx_i เป็นการบวกและการคูณมอดุโล q ตามลำดับ เราสามารถตรวจสอบได้ไม่ยากนักว่า F_q^n เป็นปริภูมิเวกเตอร์บนฟิลด์ F_q มี (0, 0, ..., 0) เป็นเวกเตอร์ศูนย์ การบวกเวกเตอร์และการคูณด้วยสเกลาร์ในตัวอย่างนี้คล้าย ๆ กับในตัวอย่าง 2.2.1 ต่างกันที่การบวกและการคูณในตัวอย่างนี้เป็นการบวกและการคูณมอดุโล q

---

หมายเหตุ :

1. เพื่อความสะดวก บางครั้งเราจะแทนเวกเตอร์ $(x_1, x_2, \ldots, x_n)$ ด้วย ลำดับ $x_1\, x_2 \ldots x_n$ ในกรณีที่ไม่ทำให้เข้าใจสับสน
2. ตลอดหนังสือเล่มนี้ เมื่อกล่าวถึงปริภูมิเวกเตอร์ F_q^n บนฟิลด์ F_q เราจะหมายถึงปริภูมิเวกเตอร์ F_q^n บนฟิลด์ F_q ภายใต้การบวกเวกเตอร์และการคูณด้วยสเกลาร์ที่กำหนดในตัวอย่าง 2.2.4 นี้เท่านั้น

3. เนื่องจาก F_q^n เป็นปริภูมิเวกเตอร์ภายใต้การดำเนินการในตัวอย่าง 2.2.4 ดังนั้น F_q^n เป็นกรุปภายใต้การบวก

นิยาม 2.2.2

ให้ V เป็นปริภูมิเวกเตอร์บนฟิลด์ F ให้ W เป็นเซตย่อยของ V ถ้า W เป็นปริภูมิเวกเตอร์บนฟิลด์ F ภายใต้การดำเนินการใน V แล้ว เราจะเรียก W ว่าปริภูมิย่อยของ V

ตัวอย่าง 2.2.5 : พิจารณาปริภูมิเวกเตอร์ F_2^5 ให้

$$C = \{00000, 10110, 01011, 11101\}$$

จะเห็นว่า $C \subset F_2^5$ เราสามารถแสดงได้ไม่ยากนักว่า C เป็นปริภูมิเวกเตอร์บนฟิลด์ F_2 ภายใต้การดำเนินการบวก และการคูณด้วยสเกลาร์ที่กำหนดในตัวอย่าง 2.2.4 สำหรับ q = 2 และ n = 5 ดังนั้น C เป็นปริภูมิย่อยของ F_2^5 มี 00000 เป็นเวกเตอร์ศูนย์

ทฤษฎีบท 2.2.1

ถ้า V เป็นปริภูมิเวกเตอร์บนฟิลด์ F และ W เป็นเซตย่อยของ V ที่ไม่ใช่เซตว่าง ถ้า W มีสมบัติปิดภายใต้การบวกและการคูณด้วยสเกลาร์ที่นิยามใน V แล้ว W จะเป็นปริภูมิย่อยของ V

จากทฤษฎีบท 2.2.1 เมื่อต้องการแสดงว่า W เป็นปริภูมิย่อยของ V เราจะต้องแสดง 2 ข้อ คือ

1. W มีสมบัติปิดภายใต้การบวก
2. W มีสมบัติปิดภายใต้การคูณด้วยสเกลาร์ในฟิลด์ F

ในกรณีเฉพาะ ถ้าต้องการแสดงว่า C เป็นปริภูมิย่อยของ F_2^n เราแสดงเฉพาะข้อ 1 เพียงข้อเดียวก็พอ ทั้งนี้เพราะว่าสเกลาร์ใน F_2 มีเพียง 0 และ 1 เท่านั้น

ตัวอย่าง 2.2.6 :

1. พิจารณารหัส $C_1 = \{000, 111\}$

เห็นได้ชัดว่า C_1 เป็นปริภูมิย่อยของ F_2^3 เพราะ $C_1 \subset F_2^3$ และ C_1 มีสมบัติปิดภายใต้การบวกเวกเตอร์ นั่นคือ

$$000 + 111 = 111 \in C_1$$

2. พิจารณารหัส $C_2 = \{000, 011, 101, 110\}$ จะเห็นว่า $C_2 \subset F_2^3$ และ

$000 + 011 = 011 \in C_2$ $\quad$ $011 + 101 = 110 \in C_2$

$000 + 101 = 101 \in C_2$ $\quad$ $011 + 110 = 101 \in C_2$

$000 + 110 = 110 \in C_2$ $\quad$ $101 + 110 = 011 \in C_2$

แสดงว่า C_2 มีสมบัติปิดภายใต้การบวก ดังนั้น C_2 เป็นปริภูมิย่อยของ F_2^3

3. พิจารณา $C_3 = \{000000, 010101, 101010, 111111\}$

ในทำนองเดียวกับข้อ 1 และ 2 จะเห็นว่า $C_3 \subset F_2^6$ และ C_3 มีสมบัติปิดภายใต้การบวก เพราะว่า

$000000+010101 = 010101 \in C_3$, $\quad$ $000000+101010 = 101010 \in C_3$

$000000+111111 = 111111 \in C_3$, $\quad$ $010101+101010 = 111111 \in C_3$

$010101+111111 = 101010 \in C_3$, $\quad$ $101010+111111 = 010101 \in C_3$

ดังนั้น C_3 เป็นปริภูมิย่อยของ F_2^6

ตัวอย่าง 2.2.7 : จะเห็นว่า

$$C = \{000, 100, 001, 111\}$$

ไม่เป็นปริภูมิย่อยของ F_2^3 ทั้งนี้เพราะว่า $100 + 001 = 101$ ซึ่งไม่อยู่ใน C แสดงว่า C ไม่มีสมบัติปิดภายใต้การบวกเวกเตอร์

ข้อสังเกต :

1. เนื่องจากปริภูมิย่อยเป็นปริภูมิเวกเตอร์ ดังนั้นต้องมีเวกเตอร์ศูนย์เสมอ

2. สำหรับปริภูมิเวกเตอร์ V ใด ๆ จะมี {0} และ V เป็นปริภูมิย่อยของ V เสมอ

นิยาม 2.2.3 ให้ $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ เป็นเวกเตอร์ในปริภูมิเวกเตอร์ V เรียกเวกเตอร์ที่เขียนในรูป $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \ldots + c_k\mathbf{v}_k$ ว่าการรวมเชิงเส้นของเวกเตอร์ $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ สำหรับ $c_1, c_2, \ldots, c_k$ ที่เป็นสเกลาร์ใด ๆ

ตัวอย่าง 2.2.8 : ในปริภูมิ R^3 เนื่องจาก

$$(0, -1, -6) = (1, 0, 0) + 2(1, 1, 0) - 3(1, 1, 2)$$

ดังนั้น เวกเตอร์ $(0, -1, -6)$ เป็นการรวมเชิงเส้นของเวกเตอร์

$$\mathbf{v}_1 = (1, 0, 0),\ \mathbf{v}_2 = (1, 1, 0),\ \text{และ}\ \mathbf{v}_3 = (1, 1, 2)$$

ในที่นี้ $c_1 = 1, c_2 = 2, c_3 = -3 \in R$

ตัวอย่าง 2.2.9 : ให้ $\mathbf{v} = (1, 0, 1), \mathbf{v}_1 = (1, 2, 1), \mathbf{v}_2 = (0,1,,2), \mathbf{v}_3 = (1,1,0)$ เป็นเวกเตอร์ใน F_3^3 จะเห็นว่า

$$(0, 1, 0) = (1, 2, 1) + (0, 1, 2) + 2(1, 1, 0)$$

หรือ

$$\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2 + 2\mathbf{v}_3$$

ดังนั้น เวกเตอร์ $\mathbf{v}$ เป็นการรวมเชิงเส้นของเวกเตอร์ $\mathbf{v}_1, \mathbf{v}_2$ และ $\mathbf{v}_3$

ในที่นี้ สเกลาร์ $c_1 = 1, c_2 = 1, c_3 = 2 \in F_3$

ตัวอย่าง 2.2.10 : ให้ $\mathbf{v}_1 = (0, 1, 1), \mathbf{v}_2 = (1, 0, 1)$ เป็นเวกเตอร์ใน F_3^3 จะเห็นว่า

$$(0, 0, 0) = 0(0, 1, 1) + 0(1, 0, 1)$$

$$(1, 1, 0) = (0, 1, 1) + (1, 0, 1)$$

ดังนั้น ทั้งเวกเตอร์ $(0, 0, 0)$ และ $(1, 1, 0)$ เป็นการรวมเชิงเส้นของเวกเตอร์ $\mathbf{v}_1$ และ $\mathbf{v}_2$

นิยาม 2.2.4 ให้ $S = \{v_1, v_2, \ldots, v_k\}$ เป็นเซตของเวกเตอร์ในปริภูมิเวกเตอร์ V ถ้าทุกเวกเตอร์ใน V เป็นการรวมเชิงเส้นของเวกเตอร์ในเซต S เราจะกล่าวว่าเซต S แผ่ทั่วปริภูมิ V บางครั้งอาจบอกว่า V ก่อกำเนิดโดย S หรือ S ก่อกำเนิด V และจะเขียน $V = \langle S \rangle$ หรือ $V = \langle v_1, v_2, \ldots, v_k \rangle$

ตัวอย่าง 2.2.11 : กำหนดให้ $v_1 = (1, 0, 0)$, $v_2 = (1, 1, 0)$, และ $v_3 = (1, 1, 2)$ เป็นเวกเตอร์ใน R^3 จงแสดงว่าเวกเตอร์ $\{v_1, v_2, v_3\}$ แผ่ทั่ว R^3

วิธีทำ ให้ (a, b, c) เป็นเวกเตอร์ใด ๆ ใน R^3 เราจะแสดงว่า (a, b, c) เป็นการรวมเชิงเส้นของเวกเตอร์ v_1, v_2 และ v_3 สมมุติให้

$$(a, b, c) = c_1(1, 0, 0) + c_2(1, 1, 0) + c_3(1, 1, 2)$$

เมื่อ c_1, c_2 และ c_3 เป็นจำนวนจริงใด ๆ ดังนั้น

$$(a, b, c) = (c_1, 0c_1, 0c_1) + (c_2, c_2, 0c_2) + (c_3, c_3, 2c_3)$$

$$= (c_1 + c_2 + c_3, 0c_1 + c_2 + c_3, 0c_1 + 0c_2 + 2c_3)$$

เราได้ระบบสมการ

$$\begin{aligned} c_1 + c_2 + c_3 &= a \\ 0c_1 + c_2 + c_3 &= b \\ 0c_1 + 0c_2 + 2c_3 &= c \end{aligned}$$

ซึ่งมี c_1, c_2 และ c_3 เป็นตัวไม่รู้ค่า หาผลเฉลยของระบบสมการ ข้างบนนี้ เราได้

$$c_1 = a - b,\ c_2 = b - \frac{c}{2} \text{ และ } c_3 = \frac{c}{2}$$

จะเห็นว่า ไม่ว่า a, b และ c จะเป็นจำนวนจริงใด ๆ จะมีค่าของ c_1, c_2 และ c_3 ที่เป็นจำนวนจริงเสมอ ที่ทำให้

$$(a, b, c) = c_1(1, 0, 0) + c_2(1, 1, 0) + c_3(1, 1, 2)$$

แสดงว่าเวกเตอร์ $\{(1,0, 0), (1,1, 0), (1,1, 2)\}$ แผ่ทั่ว R^3

ตัวอย่าง 2.2.12 : ในตัวอย่าง 2.2.6 เรารู้ว่ารหัส

$$C_2 = \{000, 011, 101, 110\}$$

เป็นปริภูมิเวกเตอร์บนฟิลด์ F_2 เมื่อ $v_1 = 011$, $v_2 = 110$ จงแสดงว่า $\{v_1, v_2\}$ แผ่ทั่วปริภูมิเวกเตอร์ C_2

วิธีทำ จะเห็นว่า

$$000 = 0(011) + 0(110) = 0v_1 + 0v_2$$
$$011 = 1(011) + 0(110) = v_1 + 0v_2$$
$$110 = 0(011) + 1(110) = 0v_1 + v_2$$
$$101 = 1(011) + 1(110) = v_1 + v_2$$

แสดงว่าทุกเวกเตอร์ใน C_2 เป็นการรวมเชิงเส้นของเวกเตอร์ 011 และ 110 นั่นคือ เวกเตอร์ 011 และ 110 แผ่ทั่ว C_2 หรือ C_2 ก่อกำเนิดโดย $\{011, 110\}$ หรือเขียน

$$C_2 = \langle 011, 110 \rangle$$

ตัวอย่าง 2.2.13 : ให้ $S = \{0101, 1010, 1100\}$ เป็นเซตของเวกเตอร์ในปริภูมิเวกเตอร์ F_2^4 จงหา $\langle S \rangle$ และขนาด $|\langle S \rangle|$

วิธีทำ ในที่นี้ เราต้องการหาเซตของเวกเตอร์ที่เป็นการรวมเชิงเส้นของเวกเตอร์ใน S นั่นคือ เราหาเวกเตอร์ที่เขียนได้ในรูป

$$a(0101) + b(1010) + c(1100)$$

สำหรับ a, b, c ที่เป็นสมาชิกใด ๆ ใน F_2 จะเห็นว่าเราสามารถเลือก a, b, c แต่ละตัวได้ 2 วิธี คือเลือกเป็น 0 หรือ 1 แสดงว่าเวกเตอร์ที่อยู่ในรูป

$$a(0101) + b(1010) + c(1100)$$

มีแตกต่างกัน $2^3 = 8$ เวกเตอร์ ซึ่งได้แก่

0(0101) + 0(1010) + 0(1100) = 0000

1(0101) + 0(1010) + 0(1100) = 0101

0(0101) + 1(1010) + 0(1100) = 1010

0(0101) + 0(1010) + 1(1100) = 1100

1(0101) + 1(1010) + 0(1100) = 1111

1(0101) + 0(1010) + 1(1100) = 1001

0(0101) + 1(1010) + 1(1100) = 0110

1(0101) + 1(1010) + 1(1100) = 0011

ดังนั้น

$<S> = \{0000, 0101, 1010, 1100, 1111, 1001, 0110, 0011\}$

และ $|<S>| = 8$

ทฤษฎีบท 2.2.2

ถ้า $S = \{ v_1, v_2, \ldots, v_k \}$ เป็นเซตของเวกเตอร์ในปริภูมิ V แล้ว $<S>$ จะเป็นปริภูมิย่อยของ V

พิสูจน์ จะต้องแสดงว่า $<S>$ มีสมบัติปิดภายใต้การบวกและการคูณด้วยสเกลาร์ ให้ $x, y \in <S>$ นั่นคือ x และ y เป็นการรวมเชิงเส้นของ $v_1, v_2, \ldots, v_k$ สมมุติให้

$$x = a_1v_1 + a_2v_2 + \ldots + a_kv_k \text{ และ}$$

$$y = b_1v_1 + b_2v_2 + \ldots + b_kv_k$$

เมื่อ a_i และ b_i สำหรับ $i = 1, 2, \ldots, k$ เป็นสเกลาร์บางสเกลาร์ ดังนั้น

$$x + y = (a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \ldots + (a_k + b_k)v_k$$

และ

$$cx = (ca_1)v_1 + (ca_2)v_2 + \ldots + (ca_k)v_k$$

เป็นการรวมเชิงเส้นของ $S = \{ v_1, v_2, \ldots, v_k \}$

นั่นคือ $x + y \in <S>$ และ $cx \in <S>$ ดังนั้น จากทฤษฎีบท 2.2.1 เราสรุปได้ว่า $<S>$ เป็นปริภูมิย่อยของ V

บทแทรก 2.2.1 เซตย่อย S ของ V ก่อกำเนิด V ก็ต่อเมื่อ $\langle S \rangle = V$

ตัวอย่าง 2.2.14 :

1. จากตัวอย่าง 2.2.12 ถ้าให้ S = {011, 110} เราพบว่า $\langle S \rangle = C_2$ ดังนั้น C_2 เป็นปริภูมิย่อยของ F_2^3 ซึ่งก่อกำเนิดโดย

$$S = \{011, 110\}$$

2. $\langle S \rangle$ ในตัวอย่าง 2.2.13 เป็นปริภูมิย่อยของ F_2^4

นิยาม 2.2.5

ให้ $S = \{v_1, v_2, \ldots, v_k\}$ เป็นเซตของเวกเตอร์ในปริภูมิเวกเตอร์ V เราจะเรียก S ว่าเซตไม่อิสระเชิงเส้น ถ้ามีสเกลาร์ $c_1, c_2, \ldots, c_k$ ซึ่งทำให้

$$c_1v_1 + c_2v_2 + \ldots + c_kv_k = 0$$

โดยที่ $c_1, c_2, \ldots, c_k$ ไม่เป็น 0 ทั้งหมด และจะเรียก S ว่าเซตอิสระเชิงเส้น ถ้ามีสเกลาร์ $c_1, c_2, \ldots, c_k$ ซึ่งทำให้

$$c_1v_1 + c_2v_2 + \ldots + c_kv_k = 0$$

โดยที่ $c_1, c_2, \ldots, c_k$ ต้องเป็น 0 ทั้งหมด

ตัวอย่าง 2.2.15 : ให้ $v_1 = (1,0,0)$, $v_2 = (1,1,0)$, และ $v_3 = (1,1,2)$ เป็นเวกเตอร์ใน R^3 จงแสดงว่า $\{v_1, v_2, v_3\}$ เป็นเซตอิสระเชิงเส้น

วิธีทำ สมมุติให้ a, b, c เป็นจำนวนจริงซึ่งทำให้

$$a(1,0,0) + b(1,1,0) + c(1,1,2) = (0,0,0)$$

หรือ $$(a,0,0) + (b,b,0) + (c,c,2c) = (0,0,0)$$

$$(a + b + c, 0 + b + c, 0 + 0 + 2c) = (0,0,0)$$

$$(a + b + c, b + c, 2c) = (0,0,0)$$

เราได้ระบบสมการ

$$a + b + c = 0$$

$$b + c = 0$$

$$2c = 0$$

ซึ่งมีผลเฉลยเพียงชุดเดียว คือ $a = b = c = 0$ แสดงว่า $\{ v_1, v_2, v_3 \}$ เป็นเซตอิสระเชิงเส้น

ตัวอย่าง 2.2.16 : ในตัวอย่าง 2.2.12 ให้ $v_1 = 011$, $v_2 = 110$ เป็นเวกเตอร์ในปริภูมิ F_2^3 จงแสดงว่า $\{ v_1, v_2 \}$ เซตอิสระเชิงเส้น

วิธีทำ สมมุติให้ a, b เป็นสเกลาร์ใน F_2 ซึ่งทำให้

$$a(1, 0, 0) + b(1, 1, 0) = (0, 0, 0)$$

หรือ $$(a, 0, 0) + (b, b, 0) = (0, 0, 0)$$

$$(a + b, 0 + b , 0 + 0) = (0, 0, 0)$$

$$(a + b, b, 0) = (0, 0, 0)$$

เราได้ระบบสมการ

$$a + b = 0$$

$$b = 0$$

ผลเฉลยของระบบสมการนี้คือ $a = 0$ และ $b = 0$ ดังนั้น {011, 110} เป็นเซตอิสระเชิงเส้น

ทฤษฎีบท 2.2.3

> ถ้า S เป็นเซตของเวกเตอร์ใน V แล้ว S จะเป็นเซตไม่อิสระเชิงเส้น ก็ต่อเมื่อมีบางเวกเตอร์ใน S เป็นการรวมเชิงเส้นของเวกเตอร์อื่น ๆ ใน S

หมายเหตุ : ถ้าเวกเตอร์ศูนย์เป็นสมาชิกของเซตย่อย S ใด ๆ ของ V แล้ว S จะเป็นเซตไม่อิสระเชิงเส้น

นิยาม 2.2.6

> ให้ $S = \{v_1, v_2, \ldots, v_k\}$ เป็นเซตของเวกเตอร์ในปริภูมิเวกเตอร์ V จะเรียกเซต S ว่าฐานหลักของ V ถ้า
>
> 1. S แผ่ทั่ว V และ
> 2. S เป็นเซตอิสระเชิงเส้น

ตัวอย่าง 2.2.17 : จากตัวอย่าง 2.2.11 เราพบว่า {(1,0, 0), (1,1, 0), (1,1, 2)} แผ่ทั่ว R^3 และจากตัวอย่าง 2.2.15 พบว่า {(1,0, 0), (1,1, 0), (1,1, 2)} เป็นเซตอิสระเชิงเส้น ดังนั้น {(1,0, 0), (1,1, 0), (1,1, 2)} เป็นฐานหลักของ R^3

ตัวอย่าง 2.2.18 : พิจารณาปริภูมิ C_2 = {000, 011, 101, 110} จากตัวอย่าง 2.2.12 และ 2.2.16 เรารู้ว่าเซต S = {011, 110} แผ่ทั่ว C_2 และ S เป็นเซตอิสระเชิงเส้น ดังนั้น S เป็นฐานหลักของปริภูมิ C_2 ในทำนองเดียวกันเราสามารถแสดงได้ว่า {011, 101} และ {110, 101} ก็เป็นฐานหลักของ C_2 ด้วยเช่นกัน (ลองทำเป็นแบบฝึกหัด)

ทฤษฎีบท 2.2.4

ถ้า $B = \{v_1, v_2, \ldots, v_n\}$ เป็นฐานหลักของ V แล้ว เวกเตอร์ใด ๆ ใน V จะเขียนในรูปการรวมเชิงเส้นของเวกเตอร์ใน B ได้เพียงแบบเดียวเท่านั้น

พิสูจน์ ให้ $\mathbf{x}$ เป็นเวกเตอร์ใด ๆ ใน V เนื่องจาก V ก่อกำเนิดโดย B ดังนั้น $\mathbf{x}$ เป็นการรวมเชิงเส้นของเวกเตอร์ใน B สมมุติว่าเขียน $\mathbf{x}$ ได้สองแบบ คือ

$$\mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_n\mathbf{v}_n$$

และ $$\mathbf{x} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \ldots + b_n\mathbf{v}_n$$

เมื่อ a_i และ b_i สำหรับ $i = 1, 2, \ldots, n$ เป็นสเกลาร์บางสเกลาร์ เราจะแสดงว่า $a_i = b_i$ สำหรับทุก $i = 1, 2, \ldots, n$

$$\mathbf{x} - \mathbf{x} = (a_1 - b_1)\mathbf{v}_1 + (a_2 - b_2)\mathbf{v}_2 + \ldots + (a_n - b_n)\mathbf{v}_n = \mathbf{0}$$

แต่เนื่องจาก $\{v_1, v_2, \ldots, v_n\}$ เป็นเซตอิสระเชิงเส้น และจากนิยาม 2.2.5 แสดงว่า

$$a_i - b_i = 0 \text{ สำหรับทุก } i = 1, 2, \ldots, n$$

ดังนั้น $a_i = b_i$ สำหรับทุก $i = 1, 2, \ldots, n$ ตามต้องการ

นิยาม 2.2.7 ให้ V เป็นปริภูมิเวกเตอร์ มิติของ V คือจำนวนสมาชิกในฐานหลักของ V ซึ่งจะเขียนแทนด้วย dim(V)

ตัวอย่าง 2.2.19 : จากตัวอย่าง 2.2.17 และ 2.2.18 เราสรุปได้ว่า

$$\dim(R^3) = 3 \quad \text{และ} \quad \dim(C_2) = 2$$

ตัวอย่าง 2.2.20 : พิจารณารหัส C_3= {000000, 010101, 101010, 111111} จะเห็นว่า C_3 = <010101, 101010> เพราะว่า

$$000000 = 0(010101) + 0(101010)$$

$$010101 = 1(010101) + 0(101010)$$

$$101010 = 0(010101) + 1(101010)$$

$$111111 = 1(010101) + 1(101010)$$

และ S = {010101, 101010} เป็นเซตอิสระเชิงเส้น เพราะไม่มีเวกเตอร์ใดเป็นพหุคูณของอีกเวกเตอร์หนึ่ง ดังนั้น S เป็นฐานหลักของ C_3 และ $\dim(C_3) = 2$

ทฤษฎีบท 2.2.5 ถ้า B = $\{v_1, v_2, \ldots, v_n\}$ เป็นฐานหลักของ V แล้ว ฐานหลักอื่น ๆ ของ V จะมี n เวกเตอร์เท่ากัน

2.3 เมทริกซ์ (Matrix)

ในที่นี้ จะถือว่าผู้อ่านมีความรู้พื้นฐานเกี่ยวกับเมทริกซ์แล้ว โดยเฉพาะเรื่องการดำเนินการตามแถวบนเมทริกซ์ ซึ่งเป็นเรื่องที่สามารถหาอ่านได้จากหนังสือพีชคณิตเชิงเส้นทั่วไป ในที่นี้จะกล่าวถึงเมทริกซ์พิเศษชนิดหนึ่งที่เรียกว่า ***วองแดร์มงด์เมทริกซ์*** ซึ่งต้องใช้ในการศึกษาเรื่องรหัส BCH ในบทที่ 6

วองแดร์มงด์เมทริกซ์ขนาด s x s คือเมทริกซ์ที่อยู่ในรูป

$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{s-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{s-1} \\ & & \vdots & & \\ 1 & \alpha_s & \alpha_s^2 & \dots & \alpha_s^{s-1} \end{bmatrix}$$

ดังนั้น ดีเทอร์มิแนนต์ของวองแดร์มงด์เมทริกซ์ คือ

$$D_s = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{s-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{s-1} \\ & & \vdots & & \\ 1 & \alpha_s & \alpha_s^2 & \dots & \alpha_s^{s-1} \end{vmatrix}$$

$$= \prod_{i>j} (\alpha_i - \alpha_j)$$

ตัวอย่าง 2.3.1 :

1. $D_2 = \begin{vmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{vmatrix} = \alpha_2 - \alpha_1$

2. $D_3 = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 1 & \alpha_2 - \alpha_1 & \alpha_2^2 - \alpha_1\alpha_2 \\ 1 & \alpha_3 - \alpha_1 & \alpha_3^2 - \alpha_1\alpha_3 \end{vmatrix}$

$$= \begin{vmatrix} \alpha_2 - \alpha_1 & \alpha_2^2 - \alpha_1\alpha_2 \\ \alpha_3 - \alpha_1 & \alpha_3^2 - \alpha_1\alpha_3 \end{vmatrix}$$

$$= (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1) \begin{vmatrix} 1 & \alpha_2 \\ 1 & \alpha_3 \end{vmatrix}$$

$$= (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$$

แบบฝึกหัด 2

1. ให้ G เป็นเซต จงพิจารณาว่า G เป็นกรุปภายใต้การดำเนินการที่กำหนดให้ในแต่ละข้อต่อไปนี้ หรือไม่

   1.1 G เป็นเซตของจำนวนเต็ม และ $a \cdot b = a - b$

   1.2 G เป็นเซตของจำนวนเต็ม และ $a \cdot b = a + b + ab$

2. จงพิจารณาว่าแต่ละข้อต่อไปนี้เป็นจริงหรือไม่

   2.1 $13 \equiv 1 \pmod 2$ 2.2 $91 \equiv 0 \pmod{13}$

3. จงพิจารณาว่าจำนวนเต็มที่กำหนดให้แต่ละคู่ต่อไปนี้ลงรอยกันมอดุโล 7 หรือไม่

   3.1 0, 42 3.2 –9, 5 3.3 –1, 553

4. ใน $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ จงหาตัวผกผันของสมาชิกแต่ละตัวที่ไม่ใช่ 0

   4.1 ภายใต้การดำเนินการบวก

   4.2 ภายใต้การดำเนินการคูณ

5. ใน $\mathbf{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ จงหาตัวผกผันของสมาชิกแต่ละตัวที่ไม่ใช่ 0

   5.1 ภายใต้การดำเนินการบวก

   5.2 ภายใต้การดำเนินการคูณ

6. จงแสดงว่าเซต $S = \{0\}$ เป็นปริภูมิย่อยของ F_q^n และ F_q^n เป็นปริภูมิย่อยของตัวเอง

7. จงแสดงว่าเซต S ในแต่ละข้อต่อไปนี้เป็นปริภูมิย่อยของปริภูมิเวกเตอร์ที่ระบุหรือไม่

   7.1 $S = \{\mathbf{x} \in F_2^n \mid$ ตำแหน่งแรกของ $\mathbf{x}$ เป็น $0\}$

   7.2 $S = \{\mathbf{x} = x_1x_2 \ldots x_n \in F_2^n \mid x_1 = x_n\}$

8. จงแสดงว่าเซต S ในแต่ละข้อต่อไปนี้เป็นปริภูมิย่อยของปริภูมิเวกเตอร์ที่ระบุหรือไม่

   8.1 $S = \{ 000, 100, 200, 010, 020, 110, 120, 210, 220\}$ ใน F_3^3

   8.2 $S = \{000, 123, 241, 314, 432\}$ ใน F_5^3

9. ให้ E_n เป็นเซตของเวกเตอร์ใน F_2^n ที่มีจำนวนเลข 1 ในแต่เวกเตอร์เป็นจำนวนคู่ จงพิจารณาว่า E_n เป็นปริภูมิย่อยของ F_2^n หรือไม่ เพราะเหตุใด

10. ให้ O_n เป็นเซตของเวกเตอร์ใน F_2^n ที่มีจำนวนเลข 1 ในแต่เวกเตอร์เป็นจำนวนคี่ จงพิจารณาว่า O_n เป็นปริภูมิย่อยของ F_2^n หรือไม่ เพราะเหตุใด

11. ให้ (2, 5, –6, 4), (1, 2, –1, 1), (0, 1, –4, 2) และ (1, 1, 3,–1) เป็นเวกเตอร์ใน R^4 จงแสดงว่าเวกเตอร์ (2, 5, –6, 4) เป็นการรวมเชิงเส้นของเวกเตอร์ (1, 2, –1, 1), (0, 1, –4, 2) และ (1, 1, 3, –1)

12. ให้ 1012, 1102, 2211 และ 2001 เป็นเวกเตอร์ใน F_3^4 จงแสดงว่าเวกเตอร์ 1012 เป็นการรวมเชิงเส้นของเวกเตอร์ 1012, 1102, 2211 และ 2001

13. ให้ 1110, 1011, 0010 เป็นเวกเตอร์ใน F_2^4 จงเขียน 1100 ในรูปการรวมเชิงเส้นของ 1110, 1011, 0010

14. ในแต่ละข้อต่อไปนี้ จงหา <S>

   14.1 $S = \{010, 011, 111\}$ ใน F_2^3

   14.2 $S = \{0101, 1010, 1111\}$ ใน F_2^4

   14.3 $S = \{1000, 0100, 0010, 0001\}$ ใน F_2^4

   14.4 $S = \{1102\}$ ใน F_3^4

15. จงหา |<S>| เมื่อ S คือเซตในข้อ 14.1 – 14.4

16. เซตใดต่อไปนี้เป็นเซตอิสระเชิงเส้น และเซตใดเป็นเซตไม่อิสระเชิงเส้น

    16.1 S = {101, 011,110, 010} ใน F_2^3

    16.2 S = {1101, 1110,110, 1011} ใน F_2^4

    16.3 S = {0110, 1010, 1100} ใน F_2^4

17. ให้ S เป็นสับเซตของ F_q^n ถ้าในเซต S มีเวกเตอร์ **0** จงแสดงว่า S เป็นเซตไม่อิสระเชิงเส้น

18. จงหาฐานหลักของปริภูมิ <S> เมื่อ S คือเซตต่อไปนี้

    18.1 S = {010, 011, 111} ใน F_2^3

    18.2 S = {1010, 0101, 1111} ใน F_2^4

    18.3 S = {1000, 0100, 0010, 0001} ใน F_2^4

19. ให้ C_2 = {000, 011, 101, 110} เป็นปริภูมิเวกเตอร์บนฟิลด์ F_2 จงแสดงว่า

    19.1 {011, 101} เป็นฐานหลักของ C_2

    19.2 {110, 101} เป็นฐานหลักของ C_2

20. ให้ C = <S> เมื่อ S คือเซตในข้อ 10.1, 10.2 และ 10.3 จงหา dim(C)

21. ให้ C_2 = {000000, 010101, 101010, 111111} จงหาจำนวนฐานหลักทั้งหมดของ C_2

22. จงหาดีเทอร์มิแนนต์ของวองแดร์มงด์เมทริกซ์ขนาด 4 x 4 นั่นคือ หา D_4