

MAT2450

6.8.12 Construire $\mathbb{F}_4$
addition

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

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

6.8.15 Est-ce que $M_n = (\mathbb{R}^{n \times n}, +, \cdot)$ fait un corps?

Rép. Non. Il y a plusieurs propriétés qui ne sont pas satisfaites.

Preuve préférée de Greg:

Dans un corps $\mathbb{F}$, si on a que

$a \in \mathbb{F}$ et $b \in \mathbb{F}$ et aussi $ab = 0$

alors $a = 0$ et/ou $b = 0$ (sinon $\mathbb{F}$ n'est pas un corps)

Peu importe n , on peut choisir

$$a = \begin{bmatrix} 1 & & \\ & 0 & \\ & & \ddots \end{bmatrix} \quad b = \begin{bmatrix} 0 & & \\ & 1 & \\ & & \ddots \end{bmatrix} \Rightarrow ab = \begin{bmatrix} 0 & & \\ & 0 & \\ & & \ddots \end{bmatrix}$$

$ab = 0$ mais $a \neq 0$ et $b \neq 0$ alors M_n n'est pas un corps.

Preuve préférée d'un étudiant Ré.

Pour un corps, la multiplication est commutative, donc $ab = ba$.

$$a = \begin{bmatrix} 1 & & \\ & 1 & \\ & & \ddots \end{bmatrix} \quad b = \begin{bmatrix} 1 & & \\ & 0 & \\ & & \ddots \end{bmatrix} \Rightarrow ab = \begin{bmatrix} 1 & 0 & \\ & 0 & \\ & & \ddots \end{bmatrix} \quad ba = \begin{bmatrix} 1 & 1 & \\ & 0 & \\ & & \ddots \end{bmatrix}$$

$ab \neq ba \Rightarrow M_n$ n'est pas un corps.

17. a) Soit $\mathbb{F}_3$ le corps à trois éléments. Il y a neuf polynômes de degré 2 de la forme $x^2 + ax + b$ où $a, b \in \mathbb{F}_3$. Énumérer ces neuf polynômes et identifier les trois qui sont irréductibles. (Suggestion : commencer par énumérer les polynômes de la forme $(x + c)(x + d)$.)
- b) Afin de construire le corps à neuf éléments, on considère le quotient $\mathbb{F}_3[x]/q(x)$ où $q(x) = x^2 + 2x + 2$. Montrer que x est une racine primitive en exprimant les huit éléments $x^i, i = 1, 2, \dots, 8$, comme polynômes de degré un ou zéro.
- c) Dans la notation de b), pour quel i l'égalité $x^3 + x^5 = x^i$ est-elle juste ?

17a. $\mathbb{F}_3[x] = \{x^2 + ax + b : a, b \in \mathbb{F}_3\}$

$P(x) = x^2 + ax + b$ est réductible s'il existe $y, z \in \mathbb{F}_3$ tel que $P(x) = (x + y)(x + z)$.

$$(x + 0)(x + 0) = x^2$$

$$(x + 0)(x + 1) = x^2 + x$$

$$(x + 0)(x + 2) = x^2 + 2x$$

$$(x + 1)(x + 1) = x^2 + 2x + 1$$

$$(x + 1)(x + 2) = x^2 + 3x + 2 = x^2 + 2$$

$$(x + 2)(x + 2) = x^2 + 4x + 4 = x^2 + x + 1.$$

irr. $x^2 + x + 2$

irr. $x^2 + 2x + 2$

irr. $x^2 + 0x + 1 = x^2 + 1$

17b. Dans $\mathbb{F}_3[x]/x^2+2x+2$, le quotient
implique que $x^2+2x+2 \equiv 0$

càd. $x^2+2x+2=0$

$-2 \equiv 1$ dans $\mathbb{F}_3$

$$\Rightarrow x^2 = -2x - 2 \Rightarrow x^2 = x + 1$$

Pour un corps de 8 éléments,
 x est primitive si $(x^n = x^m \Rightarrow n=m) \quad \forall n, m \in \{1, \dots, 8\}$

Alors

$$x^1 = x$$

$$x^2 = x + 1$$

$$x^3 = x(x+1) = x^2 + x = 2x + 1$$

$$x^4 = x(2x+1) = 2x^2 + x = 2x + 2 + x = 2$$

$$x^5 = x(2) = 2x$$

$$x^6 = 2x^2 = 2x + 2$$

$$x^7 = (2x+2)x = 2x^2 + 2x = 4x + 2 = x + 2$$

$$x^8 = x(x+2) = x^2 + 2x = 1$$

$$17c. \quad x^3 + x^6 = (2x+1) + (2x) = x+1$$

$$= x^2.$$

La réponse est $i=2$.