Fondement de l'Algorithmique Algébrique (FLAG, 4I902, MSA – IAL)

CM1 : Corps finis

par Jérémy Berthomieu

Sorbonne Universités, UPMC Univ Paris 06, CNRS, INRIA
Laboratoire d'Informatique de Paris 6 (LIP6), Équipe PolSys

Équipe pédagogique

- CM (20 h): J. Berthomieu
- TD (20 h) et TME (20 h) :
  - J. Berthomieu & M. Safey El Din (UPMC SFPN)
  - G. Couteau (Polytech MAIN)

Évaluation

- Deux examens répartis :
  - Examen réparti 1 : à la moitié du semestre, 50% ;
  - Examen réparti 2 : à la fin du semestre, 50%.

Définition.

Un groupe multiplicatif $(G,\cdot)$ est un ensemble G muni d'une loi $\cdot$ vérifiant les quatre axiomes suivants :

- **Loi de composition interne :** $\forall g_1, g_2 \in G,\ g_1 \cdot g_2 = g_1\, g_2 \in G$;
- **Associativité :** $\forall g_1, g_2, g_3 \in G,\ (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$;
- **Élément neutre :** $\exists e \in G,\ \forall g \in G,\ e \cdot g = g \cdot e = g$, e est parfois noté $1_G = 1$;
- **Symétrie :** $\forall g \in G,\ \exists g' \in G,\ g\, g' = g'\, g = e$, g' est parfois noté g^{-1} et appelé inverse.

Théorème.

- L'élément neutre d'un groupe est unique.
- Le symétrique d'un élément est unique.

Remarque.

Un groupe **abélien** vérifie en plus

- **Commutativité :** $\forall g_1, g_2 \in G,\ g_1\, g_2 = g_2\, g_1$.

On peut alors (parfois) noter $+$ sa loi, $0_G = 0$ son neutre et $-g$ le symétrique ou opposé de g.

Exemples.

- Le groupe symétrique $\mathfrak{S}_n$, c'est le groupe des permutations de $\{1,\ldots,n\}$:
  - il est engendrés par les transpositions (a,b) envoyant a sur b et b sur a ;
  - il est **non abélien** pour $n \geqslant 3$: $\left\{ \begin{array}{l} (1,2)\,(1,3) = (1,3,2) \\ (1,3)\,(1,2) = (1,2,3) \end{array} \right.$.
- Le groupe abélien $\mathbb{Z}/n\,\mathbb{Z}$ des entiers modulo n.
- Le groupe des réels strictement positifs $(\mathbb{R}_+^*,\cdot)$.
- Le groupe des complexes non nuls $(\mathbb{C}^*,\cdot)$.
- Tout espace vectoriel est un groupe pour l'addition.
- Le groupe $\left(\left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{Z}\right\},\cdot\right)$.

Définition.

Un **sous-groupe** H de G est un sous-ensemble de G contenant 1 et qui est stable par $\cdot$ et passage à l'inverse.

- Le sous-groupe $\langle g_1, \ldots, g_k \rangle$ est le plus petit sous-groupe contenant $g_1, \ldots, g_k$. Il s'agit de 1 et de tous les éléments qui sont produits de $g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}$.

Théorème (de Lagrange).

Soit G un groupe fini. Si H est un sous-groupe de G, alors $|H|$ divise $|G|$.

$\rightarrow$ Soit G de cardinal n, pour tout $g \in G$, il existe $k \mid n$ tel que $x^k = x^n = 1$.

Remarque.

Un groupe est **cyclique** s'il est fini et engendré par un seul élément.

Exemples.

- $(\mathbb{R}_+^*, \cdot)$ est un sous-groupe de $(\mathbb{C}^*, \cdot)$.
- Le sous-groupe alterné $\mathfrak{A}_n$ de $\mathfrak{S}_n$, c'est le groupe des permutations paires de $\{1, \ldots, n\}$:
  - il est engendré par les 3-cycles (a, b, c) envoyant a sur b, b sur c et c sur a ;
  - il est engendré par les paires de transpositions $(a, b)\,(c, d)$ envoyant c sur d, d sur c **puis** a sur b et b sur a.
  - il est **non abélien** pour $n \geqslant 4$: $\begin{cases} (1,2,3)\,(1,2,4) = (1,3)\,(2,4) \\ (1,2,4)\,(1,2,3) = (1,4)\,(1,3) \end{cases}$.
- Les sous-groupes de $(\{1, \mathrm{i}, -1, -\mathrm{i}\}, \cdot)$ sont $(\{1\}, \cdot), (\{1, -1\}, \cdot)$.
- $\mathbb{Z}/n\,\mathbb{Z} = \langle 1 \rangle$ est **cyclique**.
- $\mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z} = \langle (1,0), (0 1) \rangle$ n'est **pas cyclique** car $\begin{cases} (1,0) + (1,0) = (0,0) \\ (1,1) + (1,1) = (0,0) \\ (0,1) + (0,1) = (0,0) \end{cases}$.
- $\mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/3\,\mathbb{Z} = \langle (1,1) \rangle$ est **cyclique**. Par le CRT, $\mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/3\,\mathbb{Z} \simeq \mathbb{Z}/6\,\mathbb{Z}$.

Définition.

Un anneau $(A, +, \cdot)$ est un ensemble A muni de deux lois $+$ et $\cdot$ tel que

- $(A, +)$ est un groupe abélien ;
- $\cdot$ vérifie les quatre axiomes suivants :
    - **Loi de composition interne :** $\forall a_1, a_2 \in A$, $a_1 \cdot a_2 = a_1\, a_2 \in A$;
    - **Associativité :** $\forall a_1, a_2, a_3 \in A$, $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$;
    - **Élément neutre :** $\exists 1 \in A$, $\forall a \in A$, $1 \cdot a = a \cdot 1 = a$;
    - **Distributivité :** $\forall a_1, a_2, a_3 \in A$, $\begin{cases} a_1 \cdot (a_2 + a_3) & = & a_1 \cdot a_2 + a_1 \cdot a_3 \\ (a_1 + a_2) \cdot a_3 & = & a_1 \cdot a_3 + a_2 \cdot a_3 \end{cases}$.

Remarque.

Un anneau **commutatif** vérifie en plus

- **Commutativité :** $\forall a_1, a_2 \in A$, $a_1\, a_2 = a_2\, a_1$.

Exemples.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux **commutatifs**.
- $\mathcal{M}_2(\mathbb{Z})$ est un anneau **non commutatif**: $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
- L'anneau $A[x] := \{\sum_{i=0}^{n} a_i x^i | a_i \in A\}$ est **le plus petit** anneau contenant A et x.
- L'anneau $A[[x]] := \{\sum_{i=0}^{\infty} a_i x^i | a_i \in A\}$.
- L'anneau $\mathbb{Z}_p := \{\sum_{i=0}^{\infty} a_i p^i | a_i \in \{0, \ldots, p-1\}\}$.

Définitions.

- Un idéal I de A est un sous-groupe de A vérifiant
  - **Absorbtion :** $\forall x \in I, a \in A$, $x\,a \in I$.
- L'anneau quotient de A par I, noté $A\,/\,I$, est l'ensemble des classes d'équivalences $a + I = \{a + i, i \in I\}$ pour $a \in A$. On parle aussi de classes modulo I.
  - On a $a + I = b + I$ si et seulement si $(b - a) \in I$.
  - L'anneau quotient est naturellement muni d'une structure d'anneau avec
    - $(a + I) + (b + I) = (a + b) + I$;
    - $(a + I)\,(b + I) = a\,b + I$.

En général, $a + I$ est noté $\bar{a}$ voire a.

Exemples.

- Les idéaux de $\mathbb{Z}$ sont les $n\,\mathbb{Z}$, les anneaux quotients sont les $\mathbb{Z}\,/\,n\,\mathbb{Z}$;
- $(x^2 + 1) = \{(x^2 + 1)\,P, P \in \mathbb{R}[x]\}$ est un idéal de $\mathbb{R}[x]$, on a $\mathbb{C} \simeq \mathbb{R}[x]\,/\,(x^2 + 1)$.

→ Les éléments de $\mathbb{R}[x]\,/\,(x^2 + 1)$ sont les polynômes de degrés au plus 1 munis de la relation $x^2 + 1 = 0$.

Définition.

La **caractéristique** d'un anneau A est

- $n > 0$ si n est le plus petit entier tel que $n \cdot 1_A := \underbrace{1 + \cdots + 1}_{n} = 0$;
- 0 sinon.

Exemples.

- La caractéristique de $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ est 0.
- La caractéristique de $\mathbb{Z}/3\mathbb{Z}$ est 3, celle de $\mathbb{Z}/6\mathbb{Z}$ est 6.

Définition.

Si pour $a \neq 0$, il existe $b \neq 0$ tel que $a\,b = 0$, alors a et b sont des **diviseurs de zéro**.

Un anneau sans diviseur de zéro est **intègre**.

Définition.

Un **corps** est un anneau $\mathbb{K}$ tel que $(\mathbb{K}^*, \cdot)$ est un groupe. Autrement dit, tout élément non nul y est inversible.

$\rightarrow$ Par définition, $(\{0\}, +, \cdot)$ est un anneau mais pas un corps.

Théorème.

- La caractéristique d'un corps est 0 ou un **nombre premier** p.
- Pour tout anneau intègre A, le **corps des fractions** $\mathbb{K}$ de A est **le plus petit** corps contenant A : c'est l'ensemble des classes d'équivalences des couples $(a, b) \in A \times A^*$ pour la relation $(a, b) \sim (c, d) \Longleftrightarrow a\,d - b\,c = 0$.

  $\rightarrow$ La classe d'équivalence de (a, b) est en général noté $\frac{a}{b}$.

Remarque.

Il s'agit de la généralisation à un anneau intègre A de la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$.

- addition : $(a, b) + (a', b') = (a\,b' + a'\,b, b\,b')$;
- multiplication : $(a, b) \cdot (a', b') = (a\,a', b\,b')$;
- inversion : si $a \neq 0$, $(a, b)^{-1} = (b, a)$.

Exemples.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\,\mathbb{Z}$ sont des corps pour p premier.
- $\mathbb{Z}, \mathbb{Z}/n\,\mathbb{Z}$ ne sont pas des corps pour n composé.
- $\mathcal{M}_2(\mathbb{Q})$ n'est pas un corps : $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- Le corps des fractions de $\mathbb{Z}$ est $\mathbb{Q} = \left\{\frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{Z}^*\right\}$!
- Le corps des fractions de $\mathbb{K}[x]$ est $\mathbb{K}(x) = \left\{\frac{P}{Q}, P \in \mathbb{K}[x], Q \in \mathbb{K}[x]^*\right\}$.
- $\left\{\begin{pmatrix} a & 2\,b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Q}\right\}$ est un corps : $\left\{\begin{array}{l} \begin{pmatrix} a & 2\,b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & 2\,d \\ d & c \end{pmatrix} = \begin{pmatrix} a\,c + 2\,b\,d & 2\,(a\,d + b\,c) \\ a\,d + b\,c & a\,c + 2\,b\,d \end{pmatrix} \\ \begin{pmatrix} a & 2\,b \\ b & a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{a}{a^2 - 2\,b^2} & \frac{-2\,b}{a^2 - 2\,b^2} \\ \frac{-b}{a^2 - 2\,b^2} & \frac{a}{a^2 - 2\,b^2} \end{pmatrix}, \ \forall (a, b) \neq (0, 0) \end{array}\right.$.
- $\left\{\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \middle| a, b, c, d \in \mathbb{R}\right\}$ est un corps **non commutatif**.

Définition.

Un corps est **fini** s'il admet un nombre fini d'éléments.

Théorème.

Soit n un entier positif. Soit $a \in \{0, \dots, n-1\}$, a est **inversible** modulo n si et seulement si a est premier avec n.

$\rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Preuve.

Si n et $a \neq 0$ sont premiers entre eux, alors par l'algorithme d'Euclide étendu, il existe $u \in \{1, \dots, n-1\}, v \in \mathbb{Z}$ tels que $a\,u + n\,v = 1$. Ainsi $a\,u = 1$ modulo n et donc u est l'inverse de a.

Réciproquement, si a et n ne sont pas premiers entre eux, alors pour tout u, $v \in \mathbb{Z}$, $1 \neq \mathrm{pgcd}(a, n) \,|\, (a\,u + n\,v)$ et donc $a\,u \neq 1 \bmod n$. Ainsi a n'admet pas d'inverse modulo n.

Théorème.

- Un corps fini est nécessairement de caractéristique positive $p > 0$.
- Un corps fini de caractéristique p possède $q = p^r$ éléments avec $r \geqslant 1$:
  - si $r = 1$, alors **l'unique** corps à p éléments est $\mathbb{F}_p = \mathbb{Z}/p\,\mathbb{Z}$.
  - sinon, il existe **un unique** corps fini **à isomorphisme près** noté $\mathbb{F}_q = \mathbb{F}_{p^r} \neq \mathbb{Z}/p^r\,\mathbb{Z}$.

Exemples.

$\mathbb{F}_2$	0	1
0	0	0
1	0	1

Exemples.

$\mathbb{F}_2$	0	1
0	0	0
1	0	1

$\mathbb{F}_4$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Exemples.

$\mathbb{F}_2$	0	1
0	0	0
1	0	1

$\mathbb{F}_4$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$\mathbb{F}_8$	0	1	β	$\beta+1$	β^2	β^2+1	$\beta^2+\beta$	$\beta^2+\beta+1$
0	0	0	0	0	0	0	0	0
1	0	1	β	$\beta+1$	β^2	β^2+1	$\beta^2+\beta$	$\beta^2+\beta+1$
β	0	β	β^2	$\beta^2+\beta$	$\beta+1$	1	$\beta^2+\beta+1$	β^2+1
$\beta+1$	0	$\beta+1$	$\beta^2+\beta$	β^2+1	$\beta^2+\beta+1$	β^2	1	β
β^2	0	β^2	$\beta+1$	$\beta^2+\beta+1$	$\beta^2+\beta$	β	β^2+1	1
β^2+1	0	β^2+1	1	β^2	β	$\beta^2+\beta+1$	$\beta+1$	$\beta^2+\beta$
$\beta^2+\beta$	0	$\beta^2+\beta$	$\beta^2+\beta+1$	1	β^2+1	$\beta+1$	β	β^2
$\beta^2+\beta+1$	0	$\beta^2+\beta+1$	β^2+1	β	1	$\beta^2+\beta$	β^2	$\beta+1$

Exemples.

$\mathbb{F}_2$	0	1
0	0	0
1	0	1

$\mathbb{F}_4$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$\mathbb{F}_8$	0	1	β	$\beta+1$	β^2	β^2+1	$\beta^2+\beta$	$\beta^2+\beta+1$
0	0	0	0	0	0	0	0	0
1	0	1	β	$\beta+1$	β^2	β^2+1	$\beta^2+\beta$	$\beta^2+\beta+1$
β	0	β	β^2	$\beta^2+\beta$	$\beta+1$	1	$\beta^2+\beta+1$	β^2+1
$\beta+1$	0	$\beta+1$	$\beta^2+\beta$	β^2+1	$\beta^2+\beta+1$	β^2	1	β
β^2	0	β^2	$\beta+1$	$\beta^2+\beta+1$	$\beta^2+\beta$	β	β^2+1	1
β^2+1	0	β^2+1	1	β^2	β	$\beta^2+\beta+1$	$\beta+1$	$\beta^2+\beta$
$\beta^2+\beta$	0	$\beta^2+\beta$	$\beta^2+\beta+1$	1	β^2+1	$\beta+1$	β	β^2
$\beta^2+\beta+1$	0	$\beta^2+\beta+1$	β^2+1	β	1	$\beta^2+\beta$	β^2	$\beta+1$

Remarque.

Il n'existe pas d'$\alpha \in \mathbb{F}_8$ tel que $\alpha(\alpha+1) = 1$.

$\rightarrow$ $\mathbb{F}_4 \not\subseteq \mathbb{F}_8$.

Exemples.

$\mathbb{F}_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Exemples.

$\mathbb{F}_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{F}_9$	0	1	2	α	$\alpha+1$	$\alpha+2$	$2\,\alpha$	$2\,\alpha+1$	$2\,\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	$2\,\alpha$	$2\,\alpha+1$	$2\,\alpha+2$
2	0	2	1	$2\,\alpha$	$2\,\alpha+2$	$2\,\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	$2\,\alpha$	2	$\alpha+2$	$2\,\alpha+2$	1	$\alpha+1$	$2\,\alpha+1$
$\alpha+1$	0	$\alpha+1$	$2\,\alpha+2$	$\alpha+2$	$2\,\alpha$	1	$2\,\alpha+1$	2	α
$\alpha+2$	0	$\alpha+2$	$2\,\alpha+1$	$2\,\alpha+2$	1	α	$\alpha+1$	$2\,\alpha$	2
$2\,\alpha$	0	$2\,\alpha$	α	1	$2\,\alpha+1$	$\alpha+1$	2	$2\,\alpha+2$	$\alpha+2$
$2\,\alpha+1$	0	$2\,\alpha+1$	$\alpha+2$	$\alpha+1$	2	$2\,\alpha$	$2\,\alpha+2$	α	1
$2\,\alpha+2$	0	$2\,\alpha+2$	$\alpha+1$	$2\,\alpha+1$	α	2	$\alpha+2$	1	$2\,\alpha$

Théorème.

Soit $p \in \mathbb{Z}$ premier. Soit $a \in \mathbb{Z}$, l'inverse de a dans $\mathbb{F}_p$ est $u \in \mathbb{Z}$ tel que $a\,u = 1 \bmod p$.

$\rightarrow$ u est obtenu grâce à l'Algorithme d'Euclide étendu appelé sur a et p.

Algorithme.

Entrée.

- Deux entiers a et b.

Sortie.

$\rightarrow$ Le pgcd d de a et b et les coefficients de Bézout u et v tels que $a\,u + b\,v = d$.

1. $r := a$, $u := 1$, $v := 0$.
2. $r' := b$, $u' := 0$, $v' := 1$.
3. **Tant que** $r' \neq 0$ **faire**
   a. $q := \mathrm{quo}\,(r, r')$.
   b. $r'' := r - q\,r'$, $r := r'$, $r' := r''$.
   c. $u'' := u - q\,u'$, $u := u'$, $u' := u''$.
   d. $v'' := v - q\,v'$, $v := v'$, $v' := v''$.
4. **Renvoyer** r, u, v.

Théorème.

Soit $p \in \mathbb{Z}$ premier. Soit $a \in \mathbb{Z}$, l'inverse de a dans $\mathbb{F}_p$ est $u \in \mathbb{Z}$ tel que $a\,u = 1 \bmod p$.

$\rightarrow$ u est obtenu grâce à l'Algorithme d'Euclide étendu appelé sur a et p.

Algorithme.

Entrée.

- Deux entiers a et b.

Sortie.

$\rightarrow$ Le pgcd d de a et b et les coefficients de Bézout u et v tels que $a\,u + b\,v = d$.

1. $s := \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix}$.
2. **Tant que** $s'[0] \neq 0$ **faire**
   a. $q := \operatorname{quo}(s[0], s'[0])$.
   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix}$.
3. **Renvoyer** s.

Exemple.

Entrée.

- $p = 251$, $a = 207$.

Sortie.

$\rightarrow$ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \operatorname{quo}(s[0], s'[0]) = 1$.

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 44 \\ 1 \\ -1 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** s.

Exemple.

Entrée.

- $p = 251$, $a = 207$.

Sortie.

$\rightarrow$ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \operatorname{quo}(s[0], s'[0]) = 4$.

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 44 \\ 1 \\ -1 \end{pmatrix} \\ \begin{pmatrix} 31 \\ -4 \\ 5 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** s.

Exemple.

Entrée.

- $p = 251$, $a = 207$.

Sortie.

$\rightarrow$ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \mathrm{quo}\,(s[0], s'[0]) = 1$.

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 31 \\ -4 \\ 5 \end{pmatrix} \\ \begin{pmatrix} 13 \\ 5 \\ -6 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** s.

Exemple.

Entrée.

- $p = 251$, $a = 207$.

Sortie.

→ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \mathrm{quo}\,(s[0], s'[0]) = 2$.

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 13 \\ 5 \\ -6 \end{pmatrix} \\ \begin{pmatrix} 5 \\ 14 \\ 17 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** s.

Exemple.

Entrée.

- $p = 251$, $a = 207$.

Sortie.

→ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \operatorname{quo}(s[0], s'[0]) = 2$.

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 5 \\ -14 \\ 17 \end{pmatrix} \\ \begin{pmatrix} 3 \\ 33 \\ -40 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** s.

Exemple.

Entrée.

- $p = 251,\ a = 207.$

Sortie.

$\rightarrow$ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \mathrm{quo}\,(s[0], s'[0]) = 1.$

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 3 \\ 33 \\ -40 \end{pmatrix} \\ \begin{pmatrix} 2 \\ -47 \\ 57 \end{pmatrix} \end{pmatrix}.$

3. **Renvoyer** s.

Exemple.

Entrée.

- $p = 251,\ a = 207.$

Sortie.

→ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \mathrm{quo}\,(s[0], s'[0]) = 1.$

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 2 \\ -47 \\ 57 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 80 \\ -97 \end{pmatrix} \end{pmatrix}.$

3. **Renvoyer** s.

Exemple.

Entrée.

- $p = 251$, $a = 207$.

Sortie.

$\rightarrow$ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \operatorname{quo}(s[0], s'[0]) = 2$.

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 \\ 80 \\ -97 \end{pmatrix} \\ \begin{pmatrix} 0 \\ -207 \\ 251 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** s.

Exemple.

Entrée.

- $p = 251$, $a = 207$.

Sortie.

→ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \mathrm{quo}\,(s[0], s'[0]) = 2$.

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 \\ 80 \\ -97 \end{pmatrix} \\ \begin{pmatrix} 0 \\ -207 \\ 251 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** $s = \begin{pmatrix} 1 \\ 80 \\ -97 \end{pmatrix}$.

Exemple.

Entrée.

- $p = 251$, $a = 207$.

Sortie.

→ L'inverse de a dans $\mathbb{F}_p$.

1. $s := \begin{pmatrix} 251 \\ 1 \\ 0 \end{pmatrix}$, $s' := \begin{pmatrix} 207 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $s'[0] \neq 0$ **faire**

   a. $q := \mathrm{quo}\,(s[0], s'[0]) = 2$.

   b. $\begin{pmatrix} s \\ s' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} s \\ s' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 \\ 80 \\ -97 \end{pmatrix} \\ \begin{pmatrix} 0 \\ -207 \\ 251 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** $s = \begin{pmatrix} 1 \\ 80 \\ -97 \end{pmatrix}$.

Donc $207^{-1} = -97 = 154 \bmod 251$.

Définition.

Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps. Si $\mathbb{K} \subseteq \mathbb{L}$, alors $\mathbb{L}$ est une **extension** de $\mathbb{K}$.

Exemples.

- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ est une extension de $\mathbb{Q}$.
- $\mathbb{R}$ est une extension de $\mathbb{Q}$.
- $\mathbb{C}$ est une extension de $\mathbb{R}$ et de $\mathbb{Q}$.
- $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{16}$ sont des extensions de $\mathbb{F}_2$.
- $\mathbb{F}_{16}$ est une extension de $\mathbb{F}_4$ mais n'est pas une extension de $\mathbb{F}_8$!
- $\mathbb{F}_8$ n'est pas une extension de $\mathbb{F}_4$.

Remarque.

Si $\mathbb{L}$ est une extension de $\mathbb{K}$, alors $\mathbb{K}$ et $\mathbb{L}$ ont la même caractéristique.

$\rightarrow$ $\mathbb{F}_{p^r}$ est une extension de $\mathbb{F}_p$ pour $r \geqslant 1$, il est donc de caractéristique p.

Définition.

Soit $\mathbb{K}$ un corps. Un polynôme $P \in \mathbb{K}[x] \setminus \{0\}$ est **irréductible** si $P = Q\,R$ avec $Q, R \in \mathbb{K}[x]$ implique que Q ou R est inversible.

Exemple.

- $(x^2 + 1) \in \mathbb{R}[x]$ est irréductible.
- $(x^2 - 2) \in \mathbb{Q}[x]$ est irréductible mais $(x^2 - 2) = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right) \in \mathbb{R}[x]$ ne l'est pas.
- $(2\,x) \in \mathbb{Q}[x]$ est irréductible car $(2\,x) = 2 \times x$ et 2 est inversible.
- $(x^2 + x + 1) \in \mathbb{F}_2[x]$ est irréductible mais $(x^2 + x + 1) = (x + \alpha)\,(x + \alpha + 1) \in \mathbb{F}_4[x]$.

Remarque.

Dans $\mathbb{K}[x]$, un polynôme P non constant est irréductible si $P = Q\,R$ implique que Q ou R est constant.

Remarque.

- Un polynôme de $\mathbb{K}[x]$ de degré 1 est nécessairement irréductible.
- Un polynôme de $\mathbb{K}[x]$ de degré 2 ou 3 est irréductible si, et seulement s'il n'a pas de racines dans $\mathbb{K}$.

Exemple.

- $(x+1) \in \mathbb{F}_2[x]$ est irréductible.
- $P = (x^2 + x + 1) \in \mathbb{F}_2[x]$ n'a pas de racine dans $\mathbb{F}_2$ car $P(0) = P(1) = 1$, P est irréductible.
- $P = (x^3 + x + 1) \in \mathbb{F}_2[x]$ n'a pas de racine dans $\mathbb{F}_2$ car $P(0) = P(1) = 1$, P est irréductible.
- $P = (x^4 + x^2 + 1) = (x^2 + x + 1)^2 \in \mathbb{F}_2[x]$ n'a pas de racine dans $\mathbb{F}_2$ car $P(0) = P(1) = 1$ mais P n'est pas irréductible.

Définitions.

- Soit A un anneau et $x \in A$. L'ensemble $(x) = \{x\, a | a \in A\}$ est un idéal de A dit **principal**.
- Soit A un anneau intègre. Si tous les **idéaux** de A sont **principaux**, alors A est **principal**.

Théorème.

Les anneaux $\mathbb{Z}$ et $\mathbb{K}[x]$, pour $\mathbb{K}$ un corps, sont **principaux**.

Exemples.

- Les idéaux de $\mathbb{Z}$ sont les $n\,\mathbb{Z} = (n) = \{n\, a | a \in \mathbb{Z}\}$.
- Les idéaux de $\mathbb{K}[x]$ sont les $(P) = P\,\mathbb{K}[x] = \{P\,A | A \in \mathbb{K}[x]\}$.

Théorème.

Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[x]$ de degré d.

- L'anneau quotient $\mathbb{K}[x]\,/\,(P)$ a naturellement une structure de $\mathbb{K}$-espace vectoriel de dimension d dont une base est $1, x, \ldots, x^{d-1}$.
- Soit $Q \in \mathbb{K}[x]$ tel que $\deg Q < d$, Q est **inversible** modulo P si et seulement si Q est premier avec P.

$\rightarrow$ $\mathbb{K}[x]\,/\,(P)$ est un corps si et seulement si P est irréductible.

Preuve.

Si P et $Q \neq 0$ sont premiers entre eux, alors par l'algorithme d'Euclide étendu, il existe $U \in \mathbb{K}[x]^*, V \in \mathbb{K}[x]$ tels que $Q\,U + P\,V = 1$. Ainsi $Q\,U = 1$ modulo P et donc U est l'inverse de Q.

Réciproquement, si Q et P ne sont pas premiers entre eux, alors pour tout $U, V \in \mathbb{K}[x]$, $1 \neq \mathrm{pgcd}(P, Q) \mid (Q\,U + P\,V)$ et donc $Q\,U \neq 1 \bmod P$. Ainsi Q n'admet pas d'inverse modulo P.

Théorème.

Soit $P\in\mathbb{K}[x]$ irréductible. Soit $A\in\mathbb{K}[x]$, l'inverse de A dans $\mathbb{K}[x]/(P)$ est $U\in\mathbb{K}[x]$ tel que $A\,U=1 \bmod p$.

$\rightarrow$ U est obtenu grâce à l'Algorithme d'Euclide étendu appelé sur A et P.

Algorithme.

Entrée.

- Deux polynômes A et B.

Sortie.

$\rightarrow$ Le pgcd D de A et B et les coefficients de Bézout U et V tels que $A\,U+B\,V=D$.

1. $R:=A$, $U:=1$, $V:=0$.
2. $R':=B$, $U':=0$, $V':=1$.
3. **Tant que** $R'\neq 0$ **faire**
   a. $Q:=\mathrm{quo}\,(R,R')$.
   b. $R'':=R-Q\,R'$, $R:=R'$, $R':=R''$.
   c. $U'':=U-Q\,U'$, $U:=U'$, $U':=U''$.
   d. $V'':=V-Q\,V'$, $V:=V'$, $V':=V''$.
4. **Renvoyer** R, U, V.

Théorème.

Soit $P \in \mathbb{K}[x]$ irréductible. Soit $A \in \mathbb{K}[x]$, l'inverse de A dans $\mathbb{K}[x]/(P)$ est $U \in \mathbb{K}[x]$ tel que $A\,U = 1 \bmod p$.

$\rightarrow$ U est obtenu grâce à l'Algorithme d'Euclide étendu appelé sur A et P.

Algorithme.

Entrée.

- Deux polynômes A et B.

Sortie.

$\rightarrow$ Le pgcd D de A et B et les coefficients de Bézout U et V tels que $A\,U + B\,V = D$.

1. $S := \begin{pmatrix} A \\ 1 \\ 0 \end{pmatrix}$, $S' := \begin{pmatrix} B \\ 0 \\ 1 \end{pmatrix}$.
2. **Tant que** $S'[0] \neq 0$ **faire**

   a. $q := \mathrm{quo}\,(S[0], S'[0])$.

   b. $\begin{pmatrix} S \\ S' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} S \\ S' \end{pmatrix}$.
3. **Renvoyer** S.

Exemple.

Entrée.

- $P = x^3 + 2$, $A = 3\,x^2 + 3\,x + 2$.

Sortie.

→ L'inverse de A dans $\mathbb{K}[x]/(P)$.

1. $S := \begin{pmatrix} x^3+2 \\ 1 \\ 0 \end{pmatrix}$, $S' := \begin{pmatrix} 3\,x^2+3\,x+2 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $S'[0] \neq 0$ **faire**

   a. $Q := \operatorname{quo}(S[0], S'[0]) = 5\,x + 2$.

   b. $\begin{pmatrix} S \\ S' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} S \\ S' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 3\,x^2+3\,x+2 \\ 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 5\,x+5 \\ 1 \\ 2\,x+5 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** S.

Exemple.

Entrée.

- $P = x^3 + 2$, $A = 3\,x^2 + 3\,x + 2$.

Sortie.

→ L'inverse de A dans $\mathbb{K}[x]\,/\,(P)$.

1. $S := \begin{pmatrix} x^3+2 \\ 1 \\ 0 \end{pmatrix}$, $S' := \begin{pmatrix} 3\,x^2+3\,x+2 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $S'[0] \neq 0$ **faire**

   a. $Q := \operatorname{quo}(S[0], S'[0]) = 2\,x$.

   b. $\begin{pmatrix} S \\ S' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} S \\ S' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 5\,x+5 \\ 1 \\ 2\,x+5 \end{pmatrix} \\ \begin{pmatrix} 2 \\ 5\,x \\ 3\,x^2+4\,x+1 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** S.

Exemple.

Entrée.

- $P = x^3 + 2$, $A = 3\,x^2 + 3\,x + 2$.

Sortie.

$\rightarrow$ L'inverse de A dans $\mathbb{K}[x]\,/\,(P)$.

1. $S := \begin{pmatrix} x^3+2 \\ 1 \\ 0 \end{pmatrix}$, $S' := \begin{pmatrix} 3\,x^2+3\,x+2 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $S'[0] \neq 0$ **faire**

   a. $Q := \mathrm{quo}\,(S[0], S'[0]) = 6\,x + 6$.

   b. $\begin{pmatrix} S \\ S' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} S \\ S' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 2 \\ 5\,x \\ 3\,x^2+4\,x+1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 5\,x^2+5\,x+1 \\ 3\,x^3+6 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** S.

Exemple.

Entrée.

- $P = x^3 + 2$, $A = 3\,x^2 + 3\,x + 2$.

Sortie.

→ L'inverse de A dans $\mathbb{K}[x]/(P)$.

1. $S := \begin{pmatrix} x^3+2 \\ 1 \\ 0 \end{pmatrix}$, $S' := \begin{pmatrix} 3\,x^2+3\,x+2 \\ 0 \\ 1 \end{pmatrix}$.

2. **Tant que** $S'[0] \neq 0$ **faire**

   a. $Q := \mathrm{quo}\,(S[0], S'[0]) = 6\,x + 6$.

   b. $\begin{pmatrix} S \\ S' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} S \\ S' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 2 \\ 5\,x \\ 3\,x^2+4\,x+1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 5\,x^2+5\,x+1 \\ 3\,x^3+6 \end{pmatrix} \end{pmatrix}$.

3. **Renvoyer** $S := \begin{pmatrix} 2 \\ 5\,x \\ 3\,x^2+4\,x+1 \end{pmatrix}$.

Exemple.

Entrée.

- $P = x^3+2,\ A = 3\,x^2+3\,x+2.$

Sortie.

→ L'inverse de A dans $\mathbb{K}[x]/(P)$.

1. $S := \begin{pmatrix} x^3+2 \\ 1 \\ 0 \end{pmatrix},\ S' := \begin{pmatrix} 3\,x^2+3\,x+2 \\ 0 \\ 1 \end{pmatrix}.$

2. **Tant que** $S'[0] \neq 0$ **faire**

   a. $Q := \mathrm{quo}\,(S[0], S'[0]) = 6\,x+6.$

   b. $\begin{pmatrix} S \\ S' \end{pmatrix} := \begin{pmatrix} 0 & \mathrm{Id}_3 \\ \mathrm{Id}_3 & -q\,\mathrm{Id}_3 \end{pmatrix} \cdot \begin{pmatrix} S \\ S' \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 2 \\ 5\,x \\ 3\,x^2+4\,x+1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 5\,x^2+5\,x+1 \\ 3\,x^3+6 \end{pmatrix} \end{pmatrix}.$

3. **Renvoyer** $S := \begin{pmatrix} 2 \\ 5\,x \\ 3\,x^2+4\,x+1 \end{pmatrix}.$

Donc $(3\,x^2+3\,x+2)^{-1} = 2^{-1}\,(3\,x^2+4\,x+1) = 5\,x^2+2\,x+4 \bmod (x^3+2).$

Exemples.

- $(x^2-2)\in\mathbb{Q}[x]$ est irréductible donc $\mathbb{Q}[x]/(x^2-2)$ est un corps :

$$\rightarrow\quad (a+b\,x)\,\frac{a-b\,x}{a^2-2\,b^2}=\frac{a^2-b^2\,x^2}{a^2-2\,b^2}=-\frac{a^2}{a^2+b^2}\,(x^2+1)+1=1 \bmod (x^2-2).$$

- $(x^2+1)\in\mathbb{R}[x]$ est irréductible donc $\mathbb{R}[x]/(x^2+1)$ est un corps :

$$\rightarrow\quad (a+b\,x)\,\frac{a-b\,x}{a^2+b^2}=\frac{a^2-b^2\,x^2}{a^2+b^2}=1-\frac{b^2}{a^2+b^2}\,(x^2+1)=1 \bmod (x^2+1).$$

- $(x^2+x+1)\in\mathbb{F}_2[x]$ est irréductible donc $\mathbb{F}_2[x]/(x^2+x+1)$ est un corps :

$$\rightarrow\quad (a+b\,x)\,\frac{a+b+b\,x}{a^2+a\,b+b^2}=\frac{a^2+a\,b+b^2\,x+b^2\,x^2}{a^2+a\,b+b^2}=1 \bmod (x^2+x+1).$$

- $(x^3+2)\in\mathbb{F}_7[x]$ est irréductible donc $\mathbb{F}_7[x]/(x^3+2)$ est un corps :

$$\rightarrow\quad (a+b\,x+c\,x^2)\,\frac{a^2+5\,b\,c+(2\,c^2+6\,a\,b)\,x+(b^2+6\,a\,c)\,x^2}{a^3+2\,b^3+4\,c^3+a\,b\,c}=1 \bmod (x^3+2).$$

- $(x^2+x)\in\mathbb{F}_2[x]$ n'est pas irréductible donc $\mathbb{F}_2[x]/(x^2+x)$ n'est pas un corps :

$$\rightarrow\quad (x+1)\,x=x^2+x=0.$$

- $(x^3+1)\in\mathbb{F}_3[x]$ n'est pas irréductible donc $\mathbb{F}_3[x]/(x^3+1)$ n'est pas un corps :

$$\rightarrow\quad (x+1)^3=x^3+1=0.$$

Proprosition.

- Soit $P \in \mathbb{K}[x]$ irréductible de degré d. L'anneau $\mathbb{K}[x]/(P)$ est un corps contenant $\mathbb{K}$.

  $\rightarrow$ $\mathbb{L} = \mathbb{K}[x]/(P)$ est une extension de $\mathbb{K}$ de degré d.

- En notant α une racine de P, on a $\mathbb{L} = \mathbb{K}[x]/(P) = \mathbb{K}(\alpha) = \{a_0 + \cdots + a_{d-1}\,\alpha^{d-1} | a_i \in \mathbb{K}\}$: le plus petit corps contenant $\mathbb{K}$ et α.

Remarque.

Bien que $\mathbb{K}[x]/(P)$ contienne **une** racine de P, il ne les contient **pas nécessairement toutes** !

Exemple.

- $\mathbb{C} = \mathbb{R}[x]/(x^2+1) = \mathbb{R}(\mathrm{i})$.
- $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$.
- $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2-2)$, $\mathbb{Q}(\mathrm{i}) = \mathbb{Q}[x]/(x^2+1)$.
- $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]/(x^3-2) \subseteq \mathbb{R}$ ne contient pas $\mathrm{e}^{2\mathrm{i}\pi/3}\sqrt[3]{2}, \mathrm{e}^{-2\mathrm{i}\pi/3}\sqrt[3]{2}$, les autres racines de x^3-2.

Théorème.

Soient $\mathbb{K}$ un corps, $\mathbb{K}'$ une extension de $\mathbb{K}$ de degré d et $\mathbb{K}''$ une extension de $\mathbb{K}'$ de degré d'. Alors $\mathbb{K}''$ est une extension de $\mathbb{K}$ de degré $d\,d'$.

$\rightarrow$ Pour $q=p^r$, $\mathbb{F}_{q^s}$ est une extension de degré s de $\mathbb{F}_q$ et une extension de degré $r\,s$ de $\mathbb{F}_p$, c'est donc $\mathbb{F}_{p^{r\,s}}$.

$\rightarrow$ Si $(e_1,\ldots,e_d)$ est une base de $\mathbb{K}'$ en tant que $\mathbb{K}$-espace vectoriel et $(f_1,\ldots,f_{d'})$ est une base de $\mathbb{K}''$ en tant que $\mathbb{K}'$-espace vectoriel, alors $(e_1\,f_1,\ldots,e_1\,f_{d'},\ldots,e_d\,f_{d'})$ est une base de $\mathbb{K}''$ en tant que $\mathbb{K}$-espace vectoriel.

Exemple.

- $\mathbb{F}_4=\mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)=\{a+b\,\alpha|a,b\in\mathbb{F}_2,\alpha^2+\alpha+1=0\}$
- $\mathbb{F}_{16}=\mathbb{F}_4[\beta]/(\beta^2+\beta+\alpha)=\{A+B\,\beta|A,B\in\mathbb{F}_4,\beta^2+\beta+1=0\}$
- $\mathbb{F}_{16}=(\mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1))[\beta]/(\beta^2+\beta+\alpha)=\{a+b\,\alpha+c\,\beta+d\,\alpha\,\beta|a,b,c,d\in\mathbb{F}_2,$ $\alpha^2+\alpha+1=\beta^2+\beta+\alpha=0\}$.

Remarque.

Soit $P = x^d + p_{d-1}\,x^{d-1} + \cdots + p_0 \in \mathbb{K}[x]$. Si $\mathbb{L} = \mathbb{K}[x]/(P)$ est corps, alors c'est un $\mathbb{K}$-espace vectoriel dont une base est $1, x, \ldots, x^{d-1}$.

→ Dans cette base, la multiplication par x a pour matrice

$$M = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -p_0 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -p_{d-1} \end{pmatrix}.$$

→ La multiplication par $a_0 + a_1\,x + \cdots + a_{d-1}\,x_{d-1}$ a pour matrice $a_0\,\mathrm{Id} + a_1\,M + \cdots + a_{d-1}\,M^{d-1}$.

Exemple.

- La multiplication par i dans $\mathbb{C} = \mathbb{R}(\mathrm{i}) = \mathbb{R}[x]/(x^2+1)$ a pour matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$,

  $\rightarrow$ $\mathbb{C} \simeq \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$.

- La multiplication par $\sqrt{2}$ dans $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2-2)$ a pour matrice $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$,

  $\rightarrow$ $\mathbb{Q}(\sqrt{2}) \simeq \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$.

- La multiplication par $\sqrt[3]{5}$ dans $\mathbb{F}_{343} = \mathbb{F}_{7^3} = \mathbb{F}_7[x]/(x^3-5)$ a pour matrice $\begin{pmatrix} 0 & 0 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$,

  $\rightarrow$ $\mathbb{F}_{343} \simeq \left\{ \begin{pmatrix} a & 5c & 5b \\ b & a & 5c \\ c & b & a \end{pmatrix} \middle| a, b \in \mathbb{F}_7 \right\}$.

- La multiplication par α dans $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)$ a pour matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$,

  $\rightarrow$ $\mathbb{F}_4 \simeq \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \middle| a, b \in \mathbb{F}_2 \right\}$.

Exemple.

- La multiplication par α dans $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)$ a pour matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$,

  $\rightarrow \quad \mathbb{F}_4 \simeq \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \middle| a, b \in \mathbb{F}_2 \right\}$.

- Dans la base $1, \alpha, \beta, \alpha\,\beta$ de $\mathbb{F}_{16} = (\mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1))[\beta]/(\beta^2+\beta+\alpha)$ sur $\mathbb{F}_2$, les matrices de multiplications par α, β et $\alpha\,\beta$ sont $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$,

  $\rightarrow \quad \mathbb{F}_{16} \simeq \left\{ \begin{pmatrix} a & b & d & c+d \\ b & a+b & c+d & c \\ c & d & a & b \\ d & c+d & b & a+b \end{pmatrix} \middle| a, b, c, d \in \mathbb{F}_2 \right\}$.

- La multiplication par γ dans $\mathbb{F}_{16} = \mathbb{F}_2[\gamma]/(\gamma^4+\gamma+1)$ a pour matrice $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$,

  $\rightarrow \quad \mathbb{F}_{16} \simeq \left\{ \begin{pmatrix} a & d & c & b \\ b & a+d & c+d & b+c \\ c & b & a+d & c+d \\ d & c & b & a+d \end{pmatrix} \middle| a, b, c, d \in \mathbb{F}_2 \right\}$.

Définition.

Soit $P = p_d x^d + \cdots + p_0 \in \mathbb{K}[x]$ et $M \in \mathcal{M}_n(\mathbb{K})$.

- P s'annule en M si $p_d M^d + \cdots + p_1 M + p_0 \mathrm{Id} = 0$;
- P est le **polynôme minimal** de M si P est **unitaire** $(p_d = 1)$ et si P est minimal pour le degré.

Exemples.

- Le polynôme minimal de $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ est $x - 2$.
- Le polynôme minimal de $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ est $(x-2)(x-3) = x^2 - 5x + 6$.
- Le polynôme minimal de $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ est $x^2 - 4x + 4$.

Théorème.

Soit $M \in \mathcal{M}_n(\mathbb{K})$ une matrice de polynôme minimal $P = x^d + p_{d-1}\, x^{d-1} + \cdots + p_0$. L'anneau $\mathbb{K}[M] = \{a_0\,\mathrm{Id} + \cdots + a_{d-1}\, M^{d-1} | a_i \in \mathbb{K}\}$ est isomorphe à $\mathbb{K}[x]/(P)$.

Exemples.

- Le polynôme minimal de $M = \begin{pmatrix} 5 & 6 & 0 \\ 3 & 2 & 4 \\ 0 & 5 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{F}_7)$ est $x^3 + 2$,

  $\to \quad \mathbb{F}_7[M] \simeq \mathbb{F}_7[x]/(x^3+2) = \mathbb{F}_{343}$.

- Le polynôme minimal de $M = \begin{pmatrix} 1 & 5 \\ 1 & 4 \end{pmatrix} \in \mathcal{M}_2(\mathbb{F}_7)$ est $x^2 + 2\,x + 6 = (x+4)\,(x+5)$,

  $\to \quad \mathbb{F}_7[M] \simeq \mathbb{F}_7[x]/(x^2+2\,x+6) \simeq \mathbb{F}_7[x]/(x+4) \times \mathbb{F}_7[x]/(x+5) \simeq \mathbb{F}_7 \times \mathbb{F}_7$.

- Le polynôme minimal de $M = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \in \mathcal{M}_2(\mathbb{F}_3)$ est $(x+2)^2 = x^2 + x + 1$,

  $\to \quad \mathbb{F}_3[M] \simeq \mathbb{F}_3[x]/(x+2)^2$.

Définition.

Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[x]$ irréductible. Soit $\mathbb{L}$ une extension de $\mathbb{K}$ contenant toutes les racines de P et soit α l'une d'entre elle. Les **conjugués** de α sont les autres racines de P.

Exemple.

- Pour $\mathbb{K} = \mathbb{Q}$, le conjugué de $\left(a + b\sqrt{2}\right) \in \mathbb{Q}\left(\sqrt{2}\right)$ est $a - b\sqrt{2}$.
- Pour $\mathbb{K} = \mathbb{R}$, le conjugué de $(a + b\,\mathrm{i}) \in \mathbb{C}$ est $a - b\,\mathrm{i}$.
- Pour $\mathbb{K} = \mathbb{F}_2$, le conjugué de $(a + b\,\alpha) \in \mathbb{F}_4 = \mathbb{F}_2[\alpha] / (\alpha^2 + 1)$ est $a + b + b\,\alpha$.
- Pour $\mathbb{K} = \mathbb{F}_2$, les conjugués de $(a + b\,\beta + c\,\beta^2) \in \mathbb{F}_8 = \mathbb{F}_2[\beta] / (\beta^3 + \beta + 1)$ sont $a + c\,\beta + (b + c)\,\beta^2$ et $a + (b + c)\,\beta + b\,\beta^2$.

Définition.

Soit $\mathbb{L} = \mathbb{K}[x]\,/\,(P)$ une extension de $\mathbb{K}$. Si toutes les racines de P sont dans $\mathbb{L}$, alors $\mathbb{L}$ est **normale**.

Remarque.

Si $\mathbb{K}$ et $\mathbb{L}$ sont finis, alors $\mathbb{L}$ est une extension **normale** de $\mathbb{K}$!

Exemple.

- Toute extension de degré 2 est normale puisque $(x-\alpha) \in \mathbb{L}[x]$ est un facteur de P et $\dfrac{P}{x-\alpha}$ est de degré 1.
- $\mathbb{F}_{16} = \mathbb{F}_2[\gamma]\,/\,(\gamma^4+\gamma+1)$ est normale

$\rightarrow$ $x^4+x+1 = (x+\gamma)\,(x+\gamma^2)\,(x+\gamma+1)\,(x+\gamma^2+1)$.

Définition.

Soit $\mathbb{L}$ une extension de $\mathbb{K}$ **normale** de degré d. Soient $\alpha_0, \ldots, \alpha_{d-1} \in \mathbb{L}$ tous conjugués sur $\mathbb{K}$. Si $(\alpha_0, \ldots, \alpha_{d-1})$ est une base de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel, alors $(\alpha_0, \ldots, \alpha_{d-1})$ est une **base normale** de $\mathbb{L}$.

Exemples.

- $\alpha, (\alpha+1) \in \mathbb{F}_4 = \mathbb{F}_2[\alpha] / (\alpha^2 + \alpha + 1)$ sont conjugués et forment clairement une base de $\mathbb{F}_4$ sur $\mathbb{F}_2$ donc $(\alpha, \alpha+1)$ est une base normale.
- $1, \beta, \beta^2 \in \mathbb{F}_8 = \mathbb{F}_8[\beta] / (\beta^3 + \beta + 1)$ forment une base de $\mathbb{F}_8$ sur $\mathbb{F}_2$ mais ne sont pas tous conjugués entre eux : 1 est son propre conjugué et les conjugués de β sont β^2, $\beta + \beta^2$.
- $\gamma, (\gamma+1), \gamma^2, (\gamma^2+1) \in \mathbb{F}_{16} = \mathbb{F}_{16}[\gamma] / (\gamma^4 + \gamma + 1)$ sont conjugués mais ne forment pas une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$ (impossible d'obtenir γ^3 comme combinaison linéaire).

Théorème.

Soit $p \in \mathbb{Z}$ premier et soit $a \in \mathbb{Z}$ premier avec p, alors $a^{p-1} = 1 \bmod p$.

$\rightarrow$ Pour tout $a \in \mathbb{F}_p$, $a^p = a$.

Théorème.

Soit $q = p^r > 1$ la puissance d'un nombre premier. Le groupe $\mathbb{F}_q^*$ est **cyclique** de cardinal $q-1$.

$\rightarrow$ Pour tout $a \in \mathbb{F}_q$, $a^q = a$.

Exemples.

- Dans $\mathbb{F}_4$, $(\alpha+1)^3 = (\alpha+1)(\alpha^2+\alpha+1)+1 = 1$.
- Dans $\mathbb{F}_8$, $\beta^7 = (\beta^4+\beta^2+\beta+1)(\beta^3+\beta+1)+1 = 1$.

Remarque.

Soit $\mathbb{F}_{p^r}$ un corps fini de caractéristique p. L'application φ: $a \in \mathbb{F}_{p^r} \to a^p \in \mathbb{F}_{p^r}$ est **l'automorphisme de Frobenius**.

Exemples.

$\mathbb{F}_4$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Remarque.

Soit $\mathbb{F}_{p^r}$ un corps fini de caractéristique p. L'application φ: $a \in \mathbb{F}_{p^r} \to a^p \in \mathbb{F}_{p^r}$ est **l'automorphisme de Frobenius**.

Exemples.

$\mathbb{F}_4$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$\mathbb{F}_4$	$0^2=0$	$1^2=1$	$\alpha^2=\alpha+1$	$(\alpha+1)^2=\alpha$
$0^2=0$	0	0	0	0
$1^2=1$	0	1	$\alpha+1$	α
$\alpha^2=\alpha+1$	0	$\alpha+1$	α	1
$(\alpha+1)^2=\alpha$	0	α	1	$\alpha+1$

Théorème.

Soit $\mathbb{F}_{q^s}$ un corps fini, extension de $\mathbb{F}_q$. Pour tout $a \in \mathbb{F}_{q^s}$, $a \in \mathbb{F}_q$ si, et seulement si $a^q = a$.

Preuve.

Le polynôme $x^q - x$ est de degré q, il admet donc au plus q racines dans $\mathbb{F}_{q^s}$. Comme $\mathbb{F}_q \subseteq \mathbb{F}_{q^s}$ et que pour tout $a \in \mathbb{F}_q$, $a^q = a$, alors les éléments de $\mathbb{F}_q$ sont exactement les racines de $x^q - x$.

Exemple.

Dans $\mathbb{F}_{16} = \mathbb{F}_2[\gamma]/(\gamma^4 + \gamma + 1)$,

$$\begin{array}{rcrcl}
(a + b\gamma + c\gamma^2 + d\gamma^3) \in \mathbb{F}_2 & \Leftrightarrow & (a + b\gamma + c\gamma^2 + d\gamma^3)^2 & = & a + c + c\gamma + (b + d)\gamma^2 + d\gamma^3 \\
 & \Leftrightarrow & (a + b\gamma + c\gamma^2 + d\gamma^3)^2 & = & a + b\gamma + c\gamma^2 + d\gamma^3 \\
 & \Leftrightarrow & b = c = d = 0 & & \\
(a + b\gamma + c\gamma^2 + d\gamma^3) \in \mathbb{F}_4 & \Leftrightarrow & (a + b\gamma + c\gamma^2 + d\gamma^3)^4 & = & a + b + c + d + (b + d)\gamma + (c + d)\gamma^2 + d\gamma^3 \\
 & \Leftrightarrow & (a + b\gamma + c\gamma^2 + d\gamma^3)^4 & = & a + b\gamma + c\gamma^2 + d\gamma^3 \\
 & \Leftrightarrow & b = c, d = 0 & &
\end{array}$$

Remarque.

$\mathbb{F}_{q^s}$ est une extension de $\mathbb{F}_{q^r}$ si, et seulement si $r \mid s$.

Exemple

Comme $6 = 2 \times 3$, $\mathbb{F}_{q^6}$ est une extension des $\mathbb{F}_{q^{2^i 3^j}}$ avec $0 \leqslant i, j \leqslant 1$.

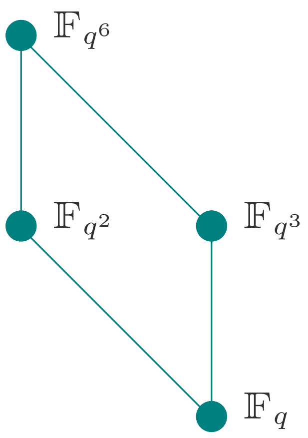

Figure 1. Quelques extensions de $\mathbb{F}_q$.

Exemple

Comme $60 = 2^2 \times 3 \times 5$, $\mathbb{F}_{q^{60}}$ est une extension des $\mathbb{F}_{q^{2^i 3^j 5^k}}$ avec $0 \leqslant i \leqslant 2$, $0 \leqslant j, k \leqslant 1$.

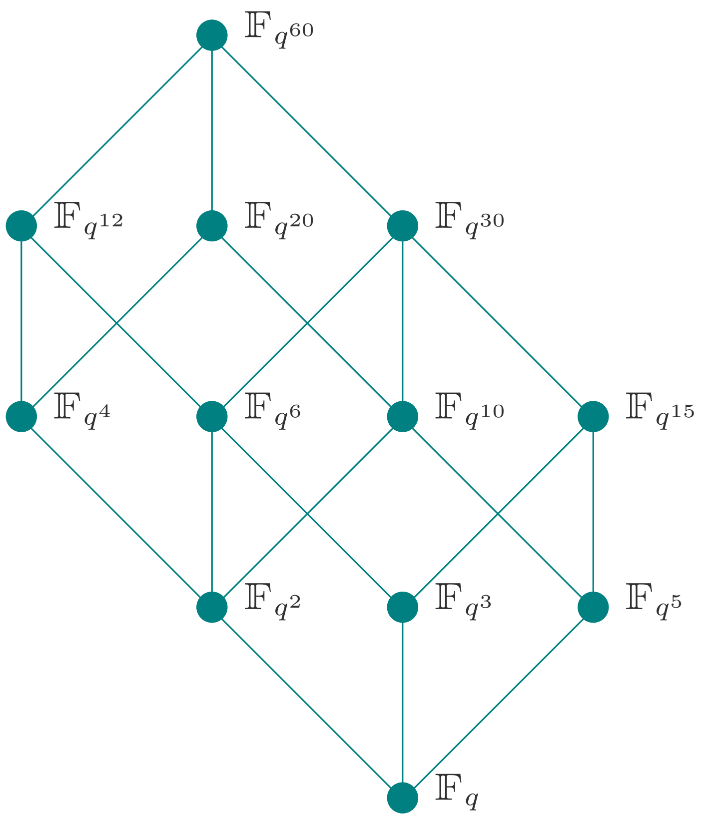

Figure 2. Quelques extensions de $\mathbb{F}_q$.

Théorème.

Soit $\mathbb{F}_{q^s}$ une extension de $\mathbb{F}_q$. Pour tout $\alpha \in \mathbb{F}_{q^s}$, les conjugués de α dans $\mathbb{F}_{q^s}$ sont

$$\alpha = \alpha^{q^0}, \alpha^q, \ldots, \alpha^{q^{s-1}}.$$

Exemples.

- Les conjugués de $\gamma \in \mathbb{F}_{16} = \mathbb{F}_2[\gamma] / (\gamma^4 + \gamma + 1)$ sont $\gamma = \gamma^{2^0}$, $\gamma^2 = \gamma^{2^1}$, $\gamma + 1 = \gamma^4 = \gamma^{2^2}$ et $\gamma^2 + 1 = \gamma^8 = \gamma^{2^3}$.
- Les conjugués de $\alpha \in \mathbb{F}_{343} = \mathbb{F}_7[\alpha] / (\alpha^3 + 2)$ sont $\alpha = \alpha^{7^0}, 4\,\alpha = \alpha^{7^1}, 2\,\alpha = \alpha^{7^2}$.

Remarque.

Soit $\alpha = \alpha^{q^0}, \ldots, \alpha^{q^{s-1}}$ une base normale de $\mathbb{F}_{q^s}$ sur $\mathbb{F}_q$. Si $a = \begin{pmatrix} a_0 \\ \vdots \\ a_{s-1} \end{pmatrix}$ dans cette base, alors $a^q = \begin{pmatrix} a_{s-1} \\ a_0 \\ \vdots \\ a_{s-2} \end{pmatrix}$ dans cette même base.

Définition.

Soit $a \in \mathbb{K}$.

- S'il existe $n \in \mathbb{N}^*$ tel que $a^n = 1$, alors a est une racine n-ième de l'unité.
- Si $n \in \mathbb{N}^*$ est le plus petit entier tel que $a^n = 1$, alors a est une racine **primitive** n-ième.

Théorème.

Si a est une racine primitive n-ième de l'unité, alors

- les racines n-ième de l'unité sont $1 = a^0, a = a^1, \ldots, a^{n-1}$;
- les autres racines primitives n-ièmes de l'unité sont les a^k avec k premier avec n.

Exemples.

- 1 et -1 sont des racines carrées de l'unité. Si $-1 \neq 1$ $(\operatorname{car} \mathbb{K} \neq 2)$, -1 est la racine primitive carrée de 1.
- $1, \mathrm{i}, \mathrm{i}^2 = -1, \mathrm{i}^3 = -\mathrm{i}$ sont les racines quatrièmes de l'unité, i et $-\mathrm{i}$ sont primitives.
- $\alpha \in \mathbb{F}_4 = \mathbb{F}_2[\alpha] / (\alpha^2 + \alpha + 1)$ est une racine cubique primitive de l'unité.

Théorème.

Toutes les racines k-ièmes de l'unité pour k divisant $q-1$ sont dans $\mathbb{F}_q$.

Exemples.

- $1, \alpha, \alpha+1$ sont les racines cubiques de l'unité dans $\mathbb{F}_4$.
- $1, 2, 4, 3$ sont les racines quatrièmes de l'unité dans $\mathbb{F}_5$, 2 et 3 sont primitives.

Remarque.

Comme $x^q - 1 = (x-1)^q$ dans $\mathbb{F}_q$, 1 est la **seule** racine q-ième de l'unité, avec multiplicité q!

$\rightarrow$ Il n'y a pas de racine primitive n p-ième de l'unité dans $\mathbb{F}_{p^r}$!

Remarque.

$(x^q - x) \in \mathbb{F}_q[x]$ se factorise en polynôme de degré 1.

→ $(x^{p^r} - x) = \prod_{\deg P | r, P \text{ irréductible, unitaire}} P$.

Exemples.

- Les polynômes irréductibles de degrés 1 ou 2 de $\mathbb{F}_2[x]$ sont $x, x+1, x^2+x+1$

  → $x^4 + x = x\,(x+1)\,(x^2+x+1)$.

- Les polynômes irréductibles de degré 1 ou 3 de $\mathbb{F}_2[x]$ sont $x, x+1, x^3+x+1, x^3+x^2+1$

  → $x^8 + x = x\,(x+1)\,(x^3+x+1)\,(x^3+x^2+1)$.

- Les polynômes irréductibles de degrés 1 ou 2 de $\mathbb{F}_3[x]$ sont x, $x+1$, $x+2$, x^2+1, x^2+x+2, $x^2+2\,x+2$

  → $x^9 - x = x\,(x+1)\,(x+2)\,(x^2+1)\,(x^2+x+2)\,(x^2+2\,x+2)$.