

Cours du jeudi 30 mars

## Algèbre

### 1. Corps de rupture et corps de décomposition

Définitions Soit  $K$  corps soit  $P(x) \in K[x]$  de degré  $> 0$

1) Il existe un corps  $K' \supset K$  où  $P$  a une racine

Il plus si  $P$  irréductible sur  $K$  si  $K'$  corps

tel que  $K' = K(x)$  et  $P(x) = 0$  alors

$$K(x) \cong K[x]/(P) \quad (\text{isomorphisme de corps})$$

on dit que  $K'$  est un corps de rupture de  $P$

$K'$  unique à isomorphisme près

2) Il existe un corps  $K' \supset K$  sur lequel le polynôme

$$P(x) = c_0 + c_1(x-\alpha_1) + \dots + c_n(x-\alpha_n)^n \quad n = \deg P$$

et  $\alpha_i \in K'$

$$\text{et } K' = K(\alpha_1, \dots, \alpha_n)$$

(on dit que  $K'$  est un corps de décomposition de  $P$  sur  $K$ )

Il plus  $K'$  unique à isomorphisme près.

Exemples. a)  $C = \mathbb{R}(i)$  est un corps de rupture de  $X^2+1$  sur  $\mathbb{R}$ .

$$f) w = e^{\frac{2i\pi}{m}}, m \geq 1$$

alors  $\mathbb{Q}(w)$  est un corps de décomposition de  $X^m-1$  sur  $\mathbb{Q}$

$$X^m-1 = (X-1)(X-w) \dots (X-w^{m-1}) \text{ et } \mathbb{Q}(1, w, \dots, w^{m-1}) = \mathbb{Q}(w)$$

c)  $\mathbb{Q}(\sqrt[3]{2})$  est un corps de rupture de  $X^3-2$  sur  $\mathbb{Q}$ .

mais non de décomposition.

$\mathbb{Q}(\sqrt[3]{2}, j)$  est un corps de décomposition de  $X^3-2$  sur  $\mathbb{Q}$

$$\text{où } j = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \text{ car } X^3-2 = (X-\sqrt[3]{2})(X-j\sqrt[3]{2})(X-j^2\sqrt[3]{2})$$

$$\text{et } \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, j)$$

Théorème 1) Si  $P$  irréductible alors  $K[X]/(P)$  est un corps

car l'idéal  $(P)$  maximal dans  $K[x]$ .

$$K \xrightarrow{x \mapsto x \pmod{P}} K[X]/(P) \quad \text{injectif.}$$

$$x \mapsto x \pmod{P}$$

Donc on peut identifier  $K$  à un sous-corps de  $K' = K[X]/(P)$

Si on pose  $\alpha := \bar{X} = X \bmod P \in K'$ , on a  $K' = K[\bar{x}] = K(\alpha)$ ,  
et  $P(\alpha) = P(\bar{X}) = \overline{P(X)} = 0 \bmod P$ .

Réiproquement si  $L$  corps tel que  $L = K(\alpha)$  où  $P(\alpha) = 0$

alors  $K[X] \xrightarrow{\varphi} L$

$$a_0 + a_1 X + \dots + a_d X^d \mapsto a_0 + a_1 \alpha + \dots + a_d \alpha^d$$

$a_i \in K$

morphisme d'anneaux de noyau  $(P)$

( $(P) \subset \text{Ker } \varphi$ ,  $(P)$  maximal  $\Rightarrow \text{Ker } \varphi = (P)$  ou ~~(P)~~  
car  $\varphi(1) = 1 \neq 0$ )

Donc  $K[X]/(P) \cong \text{Im } \varphi = K[\alpha] = K(x)$

2) Réurrence sur le degré.

## 2) Caractéristique

Soit  $K$  corps.

Le morphisme  $\mathbb{Z} \xrightarrow{\varphi} K$  est d'anneaux  
 $m \longmapsto \underbrace{1+1+\dots+1}_{m \text{ fois}}$

et de noyau  $(0)$  ou  $p\mathbb{Z}$  pour un premier  $p$  car  $\mathbb{Z}/\text{Ker } \varphi \hookrightarrow K$   
 intègre

Définition Si  $\text{Ker } \varphi = (0)$  on dit que  $K$  de caractéristique nulle

Si  $\text{Ker } \varphi = p\mathbb{Z}$  on dit que  $K$  est de caractéristique  $p$ .

Remarques. 1) Si  $\text{car}(K) = 0$ , alors  $\mathbb{Q} \subset K$ .

2) Si  $\text{car}(K) = p$ , alors  $\mathbb{Z}/p\mathbb{Z} \subset K$

ex.  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2}), \mathbb{R}(x), \dots$  sont de caractéristique nulle

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{F}_p(x)$  sont de caractéristique  $p$ .

$\mathbb{Z}[\sqrt{2}]/(3)$  de caractéristique 3

## 3) Corps finis

Exemple  $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ ,  $\mathbb{Z}^{[i]}/(7)$  corps de cardinal  $7^i$ ,  $\mathbb{Z}[\zeta]/(2)$  corps

de cardinal 4,  $\mathbb{Z}[\sqrt{2}]/(3)$  corps de cardinal 9.

Théorème 1) Si  $K$  corps fini, alors  $(K, +) \cong (\mathbb{Z}/p\mathbb{Z})^m, +)$  comme groupe

(pour un nombre premier  $p$  et un entier  $n \geq 1$ )

En particulier  $|K| = p^m$ .

2)  $\forall p$  premier,  $\forall n \geq 1$ , il existe  $K$  corps fini de cardinal  $p^n$

de plus si  $K, K'$  corps de cardinal  $p^n$ , alors  $K \cong K'$

Démonstration)  $\text{car}(K) = p$  premier et  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow K$  injectif

Donc  $K$  est un  $\mathbb{F}_p$ -espace vectoriel de dimension finie  $= m$

$$\Rightarrow (K, +) \cong (\mathbb{F}_p^m, +)$$

$$Ex. \quad \mathbb{Z}[\sqrt{2}] / \langle 3 \rangle = \mathbb{F}_3 \oplus \mathbb{F}_3 \cdot \sqrt{2} \cong \mathbb{F}_3^2$$

Morphisme de Frobenius. Soit  $K$  corps de caractéristique  $p > 0$ .

Alors  $f_p : K \rightarrow K$  est un morphisme de corps

$$\text{Démon. } (x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \dots + \binom{p}{p-1} x y^{p-1} y^p = x^p + y^p.$$

Où  $\forall 1 \leq k \leq p-1$ ,  $\binom{p}{k}$  multiple de  $p$ .

$$= \frac{1 \times 2 \times \dots \times p}{1 \times 2 \times \dots \times k \times 1 \times 2 \times \dots \times (p-k)}$$

Proposition. Si  $G \leq K^\times$  sous-groupe fini

où  $K^\times = (K \setminus \{0\}, \cdot)$  avec  $K$  corps (commutatif)

alors  $G$  cyclique.

En particulier, si  $K$  corps fini,  $K^\times$  cyclique d'ordre  $|K| - 1$

Exemples. a) Si  $U_n \leq \mathbb{C}^\times$  sous-groupe d'ordre  $n$ , alors  $U_n = \langle e^{\frac{2\pi i}{n}} \rangle$ .

$$b) (\mathbb{Z}/17\mathbb{Z})^\times = \mathbb{F}_{17}^\times = \langle 3 \rangle$$

$$\text{car } 3^2 = 9, \quad 3^4 = 81 = 13 = -4, \quad 3^8 = 16 = -1, \quad 3^{16} = 1$$

$$\text{Exo. } (\mathbb{Z}[\sqrt{2}]/(3))^{\times} = \mathbb{F}_9^{\times} = \langle \bar{1} + \sqrt{2} \rangle$$

Démo. Soit  $G \leq K^{\times}$  sous-groupe fini d'ordre  $N$

$$\text{Alors } G = \bigsqcup_{d|N} U_d \text{ où } U_d = \{ g \in G : g \text{ d'ordre } d \}$$

$$N = \sum_{d|N} |U_d| \text{ et } \forall d|N, |U_d| = 0 \text{ ou } \varphi(d)$$

En effet si  $U_d \neq \emptyset$ , soit  $x \in U_d$ ,  $x$  d'ordre  $d$  et  $\langle x \rangle = d$

Donc  $\forall y \in \langle x \rangle, y^d = 1$  donc les solutions de  
l'équation  $t^d = 1$  sont les éléments de  $\langle x \rangle$ .

En particulier,  $\forall g \in U_d, g \in \langle x \rangle \Rightarrow g = x^k$  avec  $k/d=1$

$$\text{Donc } U_d = \{ x^k : k/d=1 \} \Rightarrow |U_d| = \varphi(d).$$

$$\text{En résumé, on a } N = \sum_{d|N} |U_d| \text{ et } \forall d|N, |U_d| \leq \varphi(d)$$

$$\text{Or } \sum_{d|N} \varphi(d) = N \text{ donc } \forall d|N, |U_d| = \varphi(d)$$

$$\text{donc } |U_N| = \varphi(N) > 0$$

Il existe au moins un élément d'ordre  $N$  dans  $G$ .

Démonstration de l'unicité d'un corps de cardinal  $p^m$ .

Soit  $K$  corps fini de cardinal  $p^m$ .

$$\forall x \in K^{\times}, x^{p^m-1} = 1 \Rightarrow \forall x \in K, x^{p^m} = x$$

Soit  $P$  un facteur irréductible de  $X^{p^m} - X$  de degré  $m$ .

Comme  $X^{p^m} - X$  est scindé sur  $K$ ,  $P$  aussi.

$$\text{Donc } \exists x \in K, P(x) = 0$$

Mais alors  $\mathbb{F}_p[X] / (P)$  a pour image  $\mathbb{F}_p(x)$   
 $r(x) \mapsto r(x)$

$$\text{donc } |\mathbb{F}_p(x)| \leq |K| = p^m$$

$$\text{Or } \mathbb{F}_p[X] / (P) \cong \mathbb{F}_p(x) \Rightarrow |\mathbb{F}_p(x)| = p^m$$

$$\text{Donc } K = \mathbb{F}_p(x) \cong \mathbb{F}_p[x]/(P)$$

Justifions l'existence d'un tel \$P\$.

$$K^\times \text{ régulier} \Rightarrow \exists \alpha \in K, \quad K^\times = \langle \alpha \rangle \Rightarrow K = \mathbb{F}_p(\alpha)$$

$\Rightarrow$  le polynôme minimal de \$\alpha\$ sur \$\mathbb{F}\_p\$ est de degré  
 $[K : \mathbb{F}_p] = [K : \mathbb{F}_p] = n$

et est irréductible sur \$\mathbb{F}\_p\$. Comme il n'existe \$x^{n+1}-x=0\$  
 on a \$x^n - \alpha = 0 \Rightarrow \mathbb{F}\_p[x] | x^n - x\$.

Démonstration de l'existence d'un corps de cardinal \$\uparrow^n\$

Proposition. On note  $I_n(\mathfrak{p}) = \left\{ P \in \mathbb{F}_{\mathfrak{p}}[x] : P \text{ unitaire, irréductible}, \deg P = n \right\}$

$$x^{n+1} - x = \prod_{d|n} P$$

Remarques. 1)  $\uparrow^n = \sum_{d|n} d | I_d(\mathfrak{p})|$  (en comptant les degrés)

$$2) |I_n(\mathfrak{p})| = \sum_{d|n} \mu\left(\frac{n}{d}\right) \uparrow^d$$

où  $\mu(k) = \begin{cases} (-1)^m & \text{si } k = p_1 \cdots p_m \text{ premiers} \\ 0 & \text{sinon} \end{cases}$

$$3) |I_2(2)| = \frac{1}{2}(2^2 - 2) = 1 \quad I_2(2) = \{x^2 + x + 1\}$$

$$|I_2(3)| = \frac{1}{2}(3^2 - 3) = 3 \quad I_2(3) = \{x^2 + 1, x^2 - x + 1, x^2 + x - 1\}$$

$$|I_3(2)| = \frac{1}{3}(2^3 - 2) = 2 \quad I_3(2) = \{x^3 + x + 1, x^3 + x^2 + 1\}$$

$$|I_3(3)| = \frac{1}{3}(3^3 - 3) = 8 \quad I_3(3) = \{x^3 + x^2 - 1, x^3 - x^2 + 1, \\ x^3 + x^2 - x + 1, x^3 - x^2 - x - 1, \\ x^3 - x + 1, x^3 - x - 1\}$$

$$|I_4(2)| = \frac{1}{4}(2^4 - 2) = 3 \quad I_4(2) = \{x^4 + x + 1, x^4 + x^3 + 1, \\ x^4 + x^3 + x^2 + x + 1\}$$

Démonstration de la proposition.

lemme Soient  $a, b \in \mathbb{N}_{>0}$

Alors i)  $(X^a - 1) \wedge (X^b - 1) = X^{a \wedge b} - 1$   
ii)  $\forall p \text{ premier}, (p^a - 1) \wedge (p^b - 1) = p^{a \wedge b} - 1$

Dès lors i) si  $a = bq + r$  avec  $0 \leq r < b$

alors  $X^a - 1 = X^b - 1 + X^r - 1$   
 $= X^b \underbrace{(X^r - 1)}_{\text{multiple de } X^r - 1} + X^r - 1$  reste de la division

euclidienne de  $X^a - 1$  par  $X^r - 1$

ii) même raisonnement.

1<sup>ère</sup> étape si  $P$  irréductible sur  $\mathbb{F}_p$  et  $P \mid X^{p^n} - X$

alors  $d = \deg P \mid n$ .

Soit  $K = \mathbb{F}_p[X]/(P)$  est un corps de cardinal  $p^d$

donc  $\forall x \in K, x^{pd} - x = 0 \Rightarrow X^{pd} - X = 0 \pmod{P}$   
 $\Rightarrow P \mid X^{pd} - X$

donc  $P \mid (X^{p^n} - X) \wedge (X^{pd} - X)$   
 $\Rightarrow P \mid X \underbrace{[(X^{p^{n-1}} - 1) \wedge (X^{p^{d-1}} - 1)]}_{= X^{(p^{n-1}) \wedge (p^{d-1})} - 1 = X^{p^{n \wedge d}} - 1}$

$\Rightarrow$  Si  $\alpha \equiv X \pmod{P}, P(\alpha) = 0$  dans  $K$

$$\Rightarrow \alpha^{p^{n \wedge d}} = \alpha$$

$$\Rightarrow \forall x \in K, x^{p^{n \wedge d}} = x \quad (\text{car } K = \mathbb{F}_p[\alpha])$$

$$\Rightarrow |K| = p^d \leq p^{n \wedge d} \Rightarrow d \leq n \wedge d \Rightarrow d = n \wedge d$$

$\Rightarrow d \mid n$ .

Réiproquement si  $d \mid n$  si  $P \in \text{Id}(\mathbb{F}_p)$

alors  $K = \mathbb{F}_p[X]/(P)$  corps de cardinal  $p^d$

et  $P$  = polynôme minimal de  $x = \bar{X} = X \bmod P$  sur  $\mathbb{F}_p$ .  
 Or  $\forall x \in K, x^{p^d} - x = 0 \Rightarrow x^{p^n} - x = 0$

$$\Rightarrow P \mid X^{p^d} - X \mid X^{p^n} - X$$

(cond'n)

$$d|n \Rightarrow p^d - 1 \mid p^n - 1 \Rightarrow X^{p^d} - 1 \mid X^{p^n} - 1 \Rightarrow X^{p^d} - X \mid X^{p^n} - X$$

3<sup>e</sup> étape.  $X^{p^n} - X$  n'a pas de facteur carré dans  $\mathbb{F}_p[X]$

$$(X^{p^n} - X)' = \underbrace{p^n}_{\geq 0} X^{p^n - 1} - 1 = -1$$

$$\Rightarrow X^{p^n} - X \wedge (X^{p^n} - X)' = 1$$

$\Rightarrow$  pas de facteur carré

(en effet si  $F^2 \mid G$  alors  $F \mid G \wedge G'$ .

$$(G = F^2 Q \Rightarrow G' = 2FF'Q + F^2Q') \quad \square$$

Existence d'un polynôme irréductible de degré  $m$  sur  $\mathbb{F}_p$ .

Par l'absurde

$$\sum_{d \mid m} d | \text{Id}(p) | = p^m \text{ si } |\text{Im}(p)| = 0$$

$$\text{Alors } p^m = \sum_{\substack{d \mid m \\ d < n}} d | \text{Id}(p) | \leq \sum_{d < n} d | \text{Id}(p) | \leq \sum_{d < n} p^d = p^m - 1 < p^m$$

absurde!

$$\Rightarrow \text{Im}(p) \neq \emptyset.$$

$$\text{Soit } P(X) \in \text{Im}(p) \text{ alors } \mathbb{F}_p[X]/(P) = \text{corps de cardinal } p^m.$$

~. ~

Autre démo.  $\mathbb{F}_{p^m}$  = corps de décomposition de  $X^{p^n} - X$  sur  $\mathbb{F}_p$

## FEUILLE D'EXERCICES 2 : CORPS

**Exercice 1.** Soit  $A$  un anneau intègre. On suppose que  $A \supseteq K$ , où  $K$  est un corps et un sous-anneau de  $A$ . Montrer que  $A$  est un  $K$ -espace vectoriel. On suppose de plus qu'il est de dimension finie. Montrer que  $A$  est un corps.

**Exercice 2.** Y a-t-il une structure de corps sur  $\mathbb{Z}/4\mathbb{Z}$  dont le groupe additif sous-jacent est le groupe  $(\mathbb{Z}/4\mathbb{Z}, +)$  ?

**Exercice 3.** Soit  $K$  un corps de caractéristique  $p$ .

- (1) Montrer que l'application  $\sigma : K \rightarrow K$  définie par  $\sigma(x) = x^p$  est un morphisme de corps.
- (2) Que vaut  $\sigma$  pour  $K = \mathbb{F}_p$  ?
- (3) On suppose que  $K$  est fini, montrer qu'alors  $\sigma$  est un isomorphisme.
- (4) Montrer que ce n'est pas nécessairement vrai si  $K$  est infini.

**Exercice 4.** On considère le groupe additif  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . On le munit d'une loi qui en fait un anneau. On nomme ses éléments  $0, 1, a, b$  ( $0$  et  $1$  sont respectivement les éléments neutres pour  $+$  et  $\cdot$ ).

- (1) Montrer que  $a + b = 1$ .
- (2) On suppose qu'un des éléments, disons  $a$ , est de carré nul. Montrer qu'alors  $ab = a$  et  $b^2 = 1$ .
- (3) On suppose que  $a^2 \neq 0 \neq b^2$  mais que  $ab = 0$ . Montrer qu'alors  $a^2 = a$  et  $b^2 = b$ . Montrer que l'anneau obtenu est isomorphe à l'anneau produit  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .
- (4) On suppose maintenant que  $a^2, b^2$  et  $ab$  sont non nuls. Montrer qu'alors  $a^2 = b, b^2 = a$  et  $ab = 1$ . Montrer que l'anneau obtenu est un corps.
- (5) Montrer qu'il existe un unique (à isomorphisme près) corps à quatre éléments.

**Exercice 5.** Soit  $\mathbb{F}_2$  le corps à deux éléments. Soit  $L = \mathbb{F}_2[X]/(X^2 + X + 1)$ .

- (1) Montrer que  $L$  est un corps à quatre éléments, et écrire ses tables d'addition et de multiplication.
- (2) Vérifier que  $L$  est isomorphe au corps construit dans l'exercice précédent.
- (3) Que se passe-t-il si on remplace  $X^2 + X + 1$  par  $X^2 + 1$  ?

**Exercice 6.** Posons  $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}$ .

- (1) Montrer que  $\mathbb{Q}(i)$  est un corps.
- (2) Trouver un polyôme  $P \in \mathbb{Q}[X]$  tel que  $\mathbb{Q}(i) \simeq \mathbb{Q}[X]/(P)$ .

**Exercice 7.** A quel corps le quotient  $\mathbb{R}[X]/(X^2 + X + 1)$  est-il isomorphe ?

**Exercice 8.** Déterminer les degrés des extensions de corps suivantes :  $\mathbb{R} \subseteq \mathbb{C}$ ,  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ ,  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$  et  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, i)$ .

**Exercice 9.** Montrer que  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ ,  $\mathbb{Q}(2^{1/6}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$  et que  $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$ . (Indication : pour la dernière égalité, donner une base du  $\mathbb{Q}$ -espace vectoriel  $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ ).

**Exercice 10.** Soit  $F = X^3 + 3X - 2$  dans  $\mathbb{Q}[X]$ .

- (1) Montrer que  $\mathbb{Q}[X]/(F)$  est un corps.
- (2) Notons  $u$  la classe de  $X$  dans  $\mathbb{Q}[X]/(F)$ . Montrer que  $(1, u, u^2)$  est une  $\mathbb{Q}$ -base de  $\mathbb{Q}[X]/(F)$ .
- (3) Exprimer  $(2u^2 + u - 3)(3u^2 - 4u + 1)$  et  $(u^2 - u + 4)^{-1}$  dans cette base.
- (4) Combien  $F$  a-t-il de racines dans  $\mathbb{Q}[X]/(F)$  ?
- (5) Est-il isomorphe à un sous-corps de  $\mathbb{R}$  ?
- (6) Est-il isomorphe à un sous-corps de  $\mathbb{C}$  non contenu dans  $\mathbb{R}$  ?

#### Degré d'une extension, règle et compas

**Exercice 11.** Soit  $K/k$  une extension de corps de degré 5, engendrée par un élément  $\alpha$ . Montrer que  $\alpha^2$  engendre la même extension.

**Exercice 12.** Soit  $K$  un corps engendré sur  $k$  par deux éléments  $\alpha$  et  $\beta$  de degrés respectifs  $m$  et  $n$ . On suppose que  $m$  et  $n$  sont premiers entre eux. Montrer que  $[K : k] = mn$ .

**Exercice 13.** Soient  $\alpha, \beta \in \mathbb{C}$ . On suppose que  $\alpha + \beta$  et  $\alpha\beta$  sont algébriques. Montrer que  $\alpha$  et  $\beta$  le sont aussi.

**Exercice 14.** Peut-on construire à la règle et au compas un carré dont l'aire est égale à celle d'un triangle donné ?

**Exercice 15.** Soit  $\alpha$  une racine réelle de  $X^3 + 3X + 1$ . Peut-on construire  $\alpha$  à la règle et au compas ?

**Exercice 16.** On cherche à trisecter à la règle et au compas l'angle  $\pi/3$ . Montrer que ceci revient à construire le nombre  $\alpha = \cos(\pi/9)$ . Montrer que  $\alpha$  est racine du polynôme  $8X^3 - 6X - 1$  et conclure.

**Exercice 17.** Pour chacun des sous-corps suivants de  $\mathbb{C}$ , dire s'il contient  $i$  :

- (a)  $\mathbb{Q}(\sqrt{-2})$     (b)  $\mathbb{Q}(\sqrt[4]{-2})$     (c)  $\mathbb{Q}(\alpha)$  où  $\alpha^3 + \alpha + 1 = 0$ .

**Exercice 18.** Soit  $\alpha = \sqrt[3]{2}$ . Quel est le polynôme irréductible qui annule  $1 + \alpha^2$  sur  $\mathbb{Q}$  ?

**Exercice 19.** Quel est le polynôme irréductible qui annule  $\sqrt{3} + \sqrt{5}$  sur

- (a)  $\mathbb{Q}$     (b)  $\mathbb{Q}(\sqrt{5})$     (c)  $\mathbb{Q}(\sqrt{10})$     (d)  $\mathbb{Q}(\sqrt{15})$  ?

#### Exercice 20. Polynômes irréductibles.

- (1) Montrer que les polynômes  $X^7 + X + 1$  et  $X^6 + X^3 + 1$  sont irréductibles dans  $\mathbb{F}_2[X]$ .

- (2) Montrer que les polynômes  $X^3 + 2X + 1$ ,  $X^3 + X^2 + 2$  et  $X^4 + X^2 + 2$  sont irréductibles dans  $\mathbb{F}_3[X]$ .

**Exercice 21. Calculs dans  $\mathbb{F}_{16}$ .**

- (1) Vérifier que  $X^4 + X + 1$  est irréductible dans  $\mathbb{F}_2[X]$ .
- (2) Justifier que  $K = \mathbb{F}_2[X]/(X^4 + X + 1)$  est un corps de cardinal 16.
- (3) Soit  $x$  la classe de  $X$  dans  $K$ . Montrer que  $x$  engendre le groupe  $K^*$ .

**Exercice 22. Algèbre linéaire et Sylow.**

Soit  $\mathbb{F}_q$  un corps avec  $q = p^r$  et  $n \geq 1$ .

- (1) Déterminer la cardinal de  $\mathrm{GL}_n(\mathbb{F}_q)$ .
- (2) Montrer que l'ensemble des matrices triangulaires dont la diagonale est constituée de 1 est un  $p$ -sous-groupe de Sylow de  $\mathrm{GL}_n(\mathbb{F}_q)$ .
- (3) Soit  $G$  un groupe fini et  $S$  un  $p$ -Sylow de  $G$ . Soit  $H$  un sous-groupe de  $G$ . Montrer qu'il existe  $g \in G$  tel que  $gSg^{-1} \cap H$  est un  $p$ -Sylow de  $H$ . *Indication : utiliser l'action de  $H$  sur  $G/S$ .*
- (4) Déduire des questions précédentes l'existence d'un  $p$ -Sylow pour tout groupe.

**Exercice 23.** Soit  $P = X^4 + 2X - 2$ .

- (1) Montrer que  $P$  a exactement deux racines réelles.
- (2) Montrer que  $P$  est irréductible dans  $\mathbb{Q}[X]$ .
- (3) Montrer que la racine réelle positive de  $P$  n'est pas constructible.

**Exercice 24.** (1) Déterminer le polynôme minimal de  $\sin \frac{\pi}{9}$  dans  $\mathbb{Q}[X]$ .

- (2) En déduire que l'angle  $\frac{\pi}{3}$  n'est pas trisectable à la règle et au compas.

**Exercice 25. Résultant et Applications.**

Soit  $k$  un corps. Soit  $P$  et  $Q$  deux polynômes non constants dans  $k[X]$ . On veut un critère numérique pour décider si  $P$  et  $Q$  sont premiers entre eux.

- (1) Soit  $p$  et  $q$  les degrés de  $P$  et  $Q$  respectivement. Montrer que  $P$  et  $Q$  ne sont pas premiers entre eux si et seulement si il existe deux polynômes non nuls  $A$  et  $B$  tels que
  - (a)  $PA = QB$  ;
  - (b)  $\deg(A) < \deg(Q)$  ;
  - (c)  $\deg(B) < \deg(P)$ .
- (2) En déduire que  $P$  et  $Q$  sont premiers entre eux si et seulement si l'application

$$\begin{aligned} \mathcal{R} : \quad k_{q-1}[X] \times k_{p-1}[X] &\longrightarrow k_{p+q-1}[X] \\ (A, B) &\longmapsto AP + BQ \end{aligned}$$

n'est pas bijective.

- (3) Déterminer la matrice  $M$  de  $\mathcal{R}$  dans les bases canoniques. Le résultant  $R(P, Q)$  est par définition le déterminant de  $M$ .

**Application.** Soit  $\alpha$  et  $\beta$  deux nombres complexes algébriques sur  $\mathbb{Q}$ . Notons  $P_\alpha$  et  $P_\beta$  leurs polynômes minimaux unitaires.

- (4) Vérifier que les deux polynômes de  $\mathbb{C}[X]$ ,  $P = P_\alpha(X)$  et  $Q = P_\beta(\alpha + \beta - X)$  ont une racine commune.
- (5) Soit  $\tilde{Q} = P_\beta(T - X) \in (\mathbb{Q}(T))[X]$  et  $\tilde{P} = P_\alpha$  pensé comme un polynôme de  $(\mathbb{Q}(T))[X]$ . Montrer que  $R(\tilde{P}, \tilde{Q})$  appartient à  $\mathbb{Q}[T]$  et s'annule en  $\alpha + \beta$ .
- (6) Déterminer le polynôme minimal de  $\sqrt{2} + \sqrt{3}$ .
- (7) Trouver un polynôme annulateur de  $\pi = \alpha\beta$  en considérant  $Q = X^q P_\beta(\frac{\pi}{X})$ .

# Solution de l'exercice 5.1

Soit  $L = \mathbb{F}_2[X]/(X^2 + X + 1)$

Comme  $\deg(X^2 + X + 1) = 2$ ,  $L$  est un  $\mathbb{F}_2$ -espace vectoriel de dimension 2. Donc comme groupe,  $(L, +) \cong \mathbb{F}_2^2 \Rightarrow |L| = 4$ .

Comme  $X^2 + X + 1$  n'a pas de racine dans  $\mathbb{F}_2$ ,  $X^2 + X + 1$  est irréductible sur  $\mathbb{F}_2$  (car de degré 2). Donc l'idéal  $(X^2 + X + 1)$  est maximal dans  $\mathbb{F}_2[X]$ .

Donc  $L$  est un corps.

Soit  $x = \bar{X} = X \bmod X^2 + X + 1$ . On a  $L = \{0, 1, x, 1+x\}$

+	0	1	$x$	$1+x$
0	0	1	$x$	$1+x$
1		0	$1+x$	$x$
$x$			0	1
$1+x$				0

*	0	1	$x$	$1+x$
0	0	0	0	0
1		1	$x$	$1+x$
$x$			$1+x$	1
$1+x$				$x$

En effet:  $x^2 + x + 1 = 0 \bmod X^2 + X + 1$   
 $\Rightarrow x^2 = -1 - x$  dans  $L$   
 $= 1 + x$  car  $L$  de caractéristique 2

addition (on peut compléter par symétrie (=commutativité))      produit

## Solution de l'exercice 20

$P = X^3 + X + 1$  est irréductible sur  $\mathbb{F}_2$ .

Raisonnons par l'absurde. Si  $P$  était réductible alors  $P$  aurait un facteur irréductible de degré 1, 2 ou 3.

Or  $P$  n'a pas de racine dans  $\mathbb{F}_2$  car  $\mathbb{F}_2 = \{0, 1\}$  et  $P(0) = 1 = P(1) \neq 0$ .

Or le seul polynôme irréductible de degré 2 sur  $\mathbb{F}_2$  (unitaire) est  $X^2 + X + 1$  et  $P = (X^2 + X + 1)(X^5 + X^4 + X^3 + X) + 1 \Rightarrow X^2 + X + 1 \nmid P$

Or les seuls polynômes irréductibles de degré 3 sur  $\mathbb{F}_2$  (unitaires) sont  $X^3 + X + 1$  et  $X^3 + X^2 + 1$

et  $P = (X^3 + X + 1)(X^4 + X^2 + X + 1) + 1 \Rightarrow X^3 + X + 1 \nmid P$

$P = (X^3 + X^2 + 1)(X^4 + X^3 + X^2 + 1) + 1 \Rightarrow X^3 + X^2 + 1 \nmid P$

d'où la contradiction...

de même pour  $X^6 + X^3 + 1$ .

# Analyse fonctionnelle.

Exercice.

Soit  $f$   $2\pi$ -périodique sur  $\mathbb{R}$  tq  $f \in L^1([0, 2\pi])$

Alors  $\forall a \in \mathbb{R}$ ,  $f$  intégrable sur  $[a, a+2\pi]$  et

$$\int_a^{2\pi} f = \int_a^{a+2\pi} f$$

Solution

$$\int_a^{a+2\pi} f = \int_a^0 f + \int_0^{2\pi} f + \int_{2\pi}^{a+2\pi} f$$

Changement de variables:  $y = x - 2\pi$

$$\int_{2\pi}^{a+2\pi} f = \int_0^a f(y+2\pi) dy = \int_0^a f$$

donc  $\int_a^{a+2\pi} f = \int_a^0 f + \cancel{\int_0^a f} + \int_0^{2\pi} f$

soit  $k \in \mathbb{Z}$  tel que  
(si  $2k\pi \leq a < 2(k+1)\pi$ ,

$$\int_0^a |f| = \sum_{j=0}^{k-1} \underbrace{\int_{2j\pi}^{2(j+1)\pi} |f|}_{\int_0^{2\pi} |f|} + \underbrace{\int_{2k\pi}^a |f|}_{\int_0^{a-2k\pi} |f|} < \infty \quad \leq \int_0^{a-2k\pi} |f| < \infty$$

Noyaux

1) Noyau de Dirichlet.

Définition

$$\forall x \in \mathbb{R}, D_m(x) = \sum_{k=-n}^m e^{ikx}$$

Propriétés

0)  $D_m$   $2\pi$ -périodique

$$1) D_m(y) = \begin{cases} \frac{\sin((m+\frac{1}{2})y)}{\sin(\frac{y}{2})} & \text{si } y \notin 2\pi\mathbb{Z} \\ 2n+1 & \text{si } y \in 2\pi\mathbb{Z} \end{cases}$$

$$2^\circ) \int_0^\pi D_m(y) dy = \int_{-\pi}^0 D_m(y) dy = \pi$$

$$\text{En particulier} \quad \int_{-\pi}^\pi D_m(y) dy = \int_0^{2\pi} D_m(y) dy = 2\pi$$

3°)  $\forall f$   $2\pi$ -périodique et  $L^1([0, 2\pi])$ ,

$$\forall x, S_m(f)(x) = \sum_{k=-n}^n c_k(f) e^{ikx} = \frac{1}{2\pi} \int_0^{2\pi} f(x-y) D_m(y) dy$$

où  $\forall k \in \mathbb{Z}, c_k(f) = \frac{1}{2\pi} \int_0^{2\pi} f(t) e^{-ikt} dt$ .

Dém. 1°)

$$\begin{aligned} \sum_{k=-n}^n e^{ikx} &= \frac{e^{-inx}}{e^{inx}-1} \frac{e^{i(2n+1)x}-1}{e^{ix}-1} \quad \text{si } x \notin 2\pi\mathbb{Z} \\ &= \frac{e^{-inx}/e^{i(n+\frac{1}{2})x}}{e^{ix/2}} \frac{e^{i(n+1/2)x}-e^{-i(n+1/2)x}}{e^{ix/2}-e^{-ix/2}} \\ &= \frac{2i \sin(m+\frac{1}{2})x}{2i \sin(\frac{x}{2})} \end{aligned}$$

$$\text{si } x \in 2\pi\mathbb{Z}, \quad \sum_{k=-n}^n e^{ikx} = \sum_{k=-n}^n 1 = 2n+1$$

$$\begin{aligned}
 2^o) \quad \int_0^\pi D_m(y) dy &= \sum_{k=-n}^m \int_0^\pi e^{iky} dy \\
 &= \pi + \sum_{k=1}^n \int_0^\pi (e^{iky} + e^{-iky}) dy \\
 &= \pi + \sum_{k=1}^n \underbrace{2 \int_0^\pi \cos ky dy}_{+ \frac{2}{R} [\sin ky]_0^\pi} \\
 &\quad = 0
 \end{aligned}$$

$$\begin{aligned}
 3^o) \quad S_n(f)(x) &= \frac{1}{2\pi} \sum_{k=-n}^n e^{ikx} \int_0^{2\pi} f(t) e^{-ikt} dt \\
 &= \frac{1}{2\pi} \sum_{k=-n}^n \int_0^{2\pi} f(t) e^{ik(x-t)} dt
 \end{aligned}$$

Changement de variables  $y = x - t$

$$\begin{aligned}
 \int_0^{2\pi} f(t) e^{ik(x-t)} dt &= \int_{x-2\pi}^x f(x-y) e^{iky} dy \\
 &= \int_0^{2\pi} f(x-y) e^{iky} dy
 \end{aligned}$$

$$\text{Donc } S_n(f)(x) = \frac{1}{2\pi} \int_0^{2\pi} f(x-y) D_m(y) dy.$$

## 2) Noyaux de Fejér

$$\text{Définition. } F_n = \frac{D_0 + D_1 + \dots + D_m}{m+1}$$

$$\forall x \in \mathbb{R}, \quad T_m(f)(x) = \frac{S_0(f)(x) + \dots + S_n(f)(x)}{m+1}$$

Propriétés 1°)  $\forall y$ ,  $F_n(y) = \begin{cases} \frac{\sin^2(\frac{n+1}{2}y)}{(n+1)\sin^2(\frac{y}{2})} & \text{si } y \notin 2\pi\mathbb{Z} \\ n+1 & \text{si } y \in 2\pi\mathbb{Z} \end{cases}$

2°)  $\forall y \in \mathbb{R}$ ,  $F_n(y) \geq 0$

$$3°) \int_0^\pi F_n(y) dy = \pi, \quad \int_{-\pi}^\pi F_n(y) dy = 2\pi$$

4°)  $\forall 0 < \delta < \pi$ ,  $F_n(y) \rightarrow 0$  uniformément sur  $[-\pi, -\delta] \cup [\delta, \pi]$

$$\text{A} \int_{[-\pi, -\pi-\delta] \cup [\delta, \pi]} F_n \xrightarrow[n \rightarrow \infty]{} 0$$

$$5°) T_n(f) = \frac{1}{2\pi} \int_0^{2\pi} f(x-y) F_n(y) dy$$

Démo. 1°)  $F_n(y) = \frac{\sum_{k=0}^m (2k+1)}{m+1}$  si  $y \in 2\pi\mathbb{Z}$

$$= \frac{m+1+2 \sum_{k=0}^{m-1} k}{m+1} = m+1$$

Si  $y \notin 2\pi\mathbb{Z}$ , alors

$$F_n(y) = \frac{1}{m+1} \sum_{k=0}^m \frac{\sin(\frac{k+1}{2}y)}{\sin(\frac{y}{2})} = \frac{1}{m+1} \frac{1}{\sin(\frac{y}{2})} \operatorname{Im} \left( \sum_{k=0}^m e^{i(\frac{k+1}{2})y} \right)$$

$$\text{On } \sum_{k=0}^m e^{i(\frac{k+1}{2})y} = \frac{e^{iy/2} - 1}{e^{iy/2} - 1} = \frac{e^{iy/2}}{e^{iy/2}} \frac{e^{i(m+1)y} - 1}{e^{i(m+1)y} - 1} = \frac{e^{iy/2}}{e^{iy/2}} \frac{e^{\frac{i(m+1)y}{2}} - e^{-\frac{i(m+1)y}{2}}}{2i} = \frac{e^{iy/2}}{2i} \frac{\sin(\frac{m+1}{2}y)}{\sin(\frac{y}{2})}$$

$$\Rightarrow F_n(y) = \frac{(\sin \frac{m+1}{2}y)^2}{(m+1) \sin(\frac{y}{2})}$$

$$30) \quad \int_0^{\pi} F_n(y) dy = \frac{1}{n+1} \sum_{k=0}^n \underbrace{\int_0^{\pi} D_k(y) dy}_{\pi} \\ = \pi$$

Théorème Si  $f$  continue  $2\pi$ -périodique sur  $\mathbb{R}$  et  $f(0)=f(2\pi)$

alors  $T_n f \xrightarrow{n \rightarrow \infty} f$  uniformément.

$$\text{dimo: } T_n f - f = \frac{1}{2\pi} \int_0^{2\pi} (f(x-y) - f(x)) F_n(y) dy \\ = \frac{1}{2\pi} \int_{[-\pi, -\delta] \cup [\delta, \pi]} (f(x-y) - f(x)) F_n(y) dy + \frac{1}{2\pi} \int_{|\gamma| < \delta} (f(x-y) - f(x)) F_n(y) dy \\ \dots$$

F/N.

Prochain cours le jeudi 6 avril à 14h.