

Algèbre - Entourez l'épreuve -> Analyse

Sujet choisi : 123 Corps finis. Application

Autre sujet :

<p><u>I Généralités sur les corps</u></p> <p><u>Def 1 :</u> Un corps est un ensemble muni de deux lois internes <math>+</math> et <math>\cdot</math> tel que <math>(K, +)</math> soit un groupe abélien d'éléments neutre 0. <math>(K, \cdot)</math> soit un groupe multiplicatif de neutre 1. <math>(K, +, \cdot)</math> soit un groupe multiplicatif de neutre 1.</p> <p><u>Ex 2 :</u> <math>\mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}</math> avec <math>p</math> premier.</p> <p><u>Def 2 :</u> Morphisme de corps : une application de corps est une application d'un corps <math>K</math> vers un corps <math>L</math> qui respecte un morphisme d'anneaux.</p> <p><u>Prop 1 :</u> un morphisme de corps est injectif ou nul.</p> <p><u>Def 3 :</u> Soit <math>\varphi : K \rightarrow L</math> un morphisme de corps</p> <p><math>\varphi</math> est entièrement déterminé : <math>\forall a \in K, \varphi(a) = 0</math> ou <math>\varphi(a) = a</math> et on appelle la caractéristique de <math>K</math> 0 ou <math>m</math></p> <p><u>Prop 6 :</u> Si <math>K</math> est un corps, <math>\text{Car}(K) = 0</math> ou <math>p</math> avec <math>p</math> premier</p> <p><u>Ex 3 :</u> <math>\text{Car}(\mathbb{R}) = \text{Car}(\mathbb{Q}) = 0</math> <math>\text{Car}(\mathbb{Z}/p\mathbb{Z}) = p</math></p> <p><u>Prop 7 :</u> Soit <math>K</math> un corps. Si <math>\text{Car}(K) = p</math> alors <math>K</math> est un corps de caractéristique <math>p</math> et <math>K</math> est isomorphe à <math>\mathbb{F}_p</math>, sinon si <math>\text{Car}(K) = 0</math> alors <math>K</math> est un corps de caractéristique 0 et <math>K</math> est isomorphe à <math>\mathbb{Q}</math>.</p> <p><u>Def 4 :</u> Un corps fini est un corps de cardinal fini.</p> <p><u>Théor 10 :</u> Soit <math>K</math> un corps fini, alors il existe <math>p</math> premier et <math>n \in \mathbb{N}</math> tel que <math> K  = p^n</math></p> <p><u>II Polynômes et corps finis</u></p> <p><u>Prop 8 :</u> Soit <math>K</math> un corps fini. <math>\mathbb{F}_p</math> est un corps de cardinal <math>p</math></p> <p><u>Lemme 11 :</u> Si <math>P \in \mathbb{F}_p[X]</math> irréductible de degré <math>d</math> est un diviseur de <math>X^p - X</math></p>	<p><u>Lemme 12 :</u> Si <math>P \in \mathbb{F}_p[X]</math> est un polynôme irréductible de degré <math>m</math> et <math>P</math> est divisible de <math>X^{p^m} - X</math> alors <math>d</math> divise <math>m</math> et <math>P</math> est divisible de <math>X^{p^m} - X</math>.</p> <p><u>Théor 13 :</u> Soit <math>\mathbb{F}_q</math> un corps fini. Pour tout <math>n \in \mathbb{N}</math> il existe un polynôme irréductible de degré <math>n</math> dans <math>\mathbb{F}_q[X]</math></p> <p><u>Exercice 14 :</u> Montrez que <math>X^4 + X^2 + 1</math> est irréductible sur <math>\mathbb{F}_2[X]</math></p> <p><u>Application 15 :</u> Pour tout <math>p</math> premier et <math>n \in \mathbb{N}</math> il existe un corps de cardinal <math>p^n</math>, c'est le corps de composition de <math>n</math> fois polynôme irréductible de degré <math>n</math> sur <math>\mathbb{F}_p[X]</math></p> <p><u>Exercice 16 :</u> <math>\mathbb{F}_2[X] / (X^2 + X + 1)</math> = <math>\{0, 1, \omega, \omega^2\}</math> avec <math>\omega^2 = \omega + 1</math></p> <p><u>III Propriétés des corps finis et applications</u></p> <p>1) <math>(\mathbb{F}_q, +)</math></p> <p><u>Théor 17 :</u> <math>(\mathbb{F}_q, +)</math> est un groupe cyclique d'ordre <math> K  - 1</math></p> <p><u>Ex 18 :</u> Théorème de Fermat <math>a^q = a</math> et <math>q^{q-1} = 1</math> si <math>a \neq 0</math> dans un corps de cardinal <math>q</math></p> <p><u>Ex 19 :</u> Morphisme de <math>\mathbb{F}_q</math> : Soit <math>K \subset \mathbb{F}_q</math> et <math> K  = p</math> donc <math>K</math> est un corps fini. Appliquez le théorème de Lagrange et <math>a^p = a</math> pour tout <math>a \in K</math>. Soit <math>f(x) = x^p - x</math> et <math>f(x) = 0</math> pour tout <math>x \in K</math>. Soit <math>f(x) = (x - a_1)(x - a_2) \dots (x - a_p)</math> et <math>f(x) = x^p - x</math> donc <math>a_i = a_j</math> pour tout <math>i, j</math>. Soit <math>f(x) = x^p - x = (x - a)^p</math> et <math>f(x) = x^p - x = (x - a)^p</math> et <math>f(x) = x^p - x = (x - a)^p</math></p> <p><u>Prop 20 :</u> Deux corps de même cardinal sont isomorphes. On note donc <math>\mathbb{F}_q</math> le corps fini de cardinal <math>q</math> unique à isomorphisme près.</p> <p><u>Ex 21 :</u> <math>\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^4} \subset \dots</math></p>
--	--

le corps de composition

Algèbre - Entourez l'épreuve -> Analyse

Sujet choisi : 123 corps finis. Application

Autre sujet :

<p><u>Exemple 22</u> : Soit corps de <math>\mathbb{Z}_3</math></p> <p><u>Exemple 23</u> :</p> $\mathbb{F}_{3^2} = \mathbb{F}_3(\alpha) / \alpha^2 + \alpha + 1$ $= \mathbb{F}_3(\alpha) / \alpha^2 + \alpha + 1$ <p>2) Le Frobenius</p> <p><u>Def 24</u> : Soit <math>K</math> un corps fini et <math>p = \text{Car}(K)</math></p> <p>Soit <math>F_\alpha : K \rightarrow K</math>  <math>x \mapsto x^p</math> <math>F</math> est appelé le Frobenius</p> <p><u>Prop 25</u> : <math>F_\alpha</math> est un automorphisme de corps et <math>\text{Dern}</math> étale de corps <math>\mathbb{Z}/p\mathbb{Z}</math>.</p> <p><u>Exemple 26</u> : Soit <math>u, v \in K</math>, <math>p = \text{Car}(K)</math>      alors <math>(u+v)^p = u^p + v^p</math></p> <p><u>Appli 27</u> : Si <math>P \in K[X]</math> a une racine <math>\lambda \in K</math> alors <math>F_\alpha(\lambda)</math> est aussi racine de <math>P</math></p> <p><u>Exercice 28</u> : <math>P = X^2 - X + 1</math> irréductible de <math>\mathbb{F}_3(\alpha)</math>      Racines de <math>P</math> sont <math>(\alpha, \alpha^2, \alpha^4, \alpha^8)</math>. Montrez que les racines de <math>P</math> sont <math>(\alpha, \alpha^2, \alpha^4, \alpha^8)</math>.</p> <p>3) Corps de <math>\mathbb{F}_q</math></p> <p><u>Def 29</u> : Le symbole de Legendre sur <math>\mathbb{F}_q</math> est pour <math>a \in K</math>  <math display="block">\left(\frac{a}{q}\right) = \begin{cases} 1 &amp; \text{si } a \text{ est un carré} \\ -1 &amp; \text{si } a \text{ n'est pas un carré} \\ 0 &amp; \text{si } a = 0 \end{cases}</math></p> <p><u>Exercice 30</u> Montrez que <math>\mathcal{S}^1</math> ensemble des carrés de <math>\mathbb{F}_q</math> est de cardinal <math>q</math> si <math>q</math> est pair et <math>\frac{q-1}{2}</math> sinon</p>	
<p><u>Théor 31</u> Soit <math>a \in \mathbb{F}_q^*</math>, alors <math>(\frac{a}{q}) = a^{\frac{q-1}{2}}</math> si <math>q</math> est impair sinon <math>a</math> est toujours un carré</p> <p><u>Exemple 32</u> <math>(\frac{2}{3}) = 2^{\frac{3-1}{2}} = 2^{-1}</math> donc <math>2</math> n'est pas un carré dans <math>\mathbb{F}_3</math></p> <p><u>Exemple 33</u> Le produit de deux non-carrés est un carré dans tout <math>\mathbb{F}_q</math>. Le n'est pas le cas sur <math>\mathbb{Z} : 2 \cdot 3 = 6</math></p> <p><u>Corollaire 34</u> : si <math>p &gt; 2</math> alors <math>-1</math> est un carré dans <math>\mathbb{F}_q</math> si et seulement si <math>q \equiv 1 \pmod{4}</math></p> <p><u>Appli 35</u> Théorème des deux carrés      Un entier est somme de deux carrés si et seulement si <math>p \equiv 1 \pmod{4}</math></p> <p><u>Appli 36</u> : Il existe une infinité de nombres premiers de la forme <math>4n+1</math></p> <p><u>Exercice 37</u> l'équation <math>ax^2 + by^2 = 1</math> d'inconnues <math>(x, y) \in K^2</math> avec <math>(a, b) \notin (K^*)^2</math> admet une seule solution sur <math>K</math>.</p> <p><u>Théorème 38</u> Réciprocité quadratique      Soient <math>p, q</math> deux nombres premiers impaires distincts, alors <math>(\frac{p}{q}) (\frac{q}{p}) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}</math></p> <p><u>Application 39</u> Si <math>x^2 = \pi</math> pi arrête pi premier  <math>(\frac{2}{p}) = \pi (\frac{2}{p})</math> donc on peut calculer <math>(\frac{2}{p})</math> en fonction de <math>(\frac{p}{2})</math> pour <math>p \neq 2</math> non premier.</p> <p><u>Exemple 40</u> : <math>(\frac{12}{3}) = (\frac{-1}{3}) = -1</math> donc <math>(\frac{12}{3}) = (\frac{12}{3}) = (-1)^{\frac{12-1}{2} \frac{3-1}{2}} = (-1)^8 = 1</math> donc <math>3</math> est la somme de deux carrés de <math>\mathbb{Z}</math>.</p>	<p><u>Exemple 32</u> <math>(\frac{2}{3}) = 2^{\frac{3-1}{2}} = 2^{-1}</math> donc <math>2</math> n'est pas un carré dans <math>\mathbb{F}_3</math></p> <p><u>Exemple 33</u> Le produit de deux non-carrés est un carré dans tout <math>\mathbb{F}_q</math>. Le n'est pas le cas sur <math>\mathbb{Z} : 2 \cdot 3 = 6</math></p> <p><u>Corollaire 34</u> : si <math>p &gt; 2</math> alors <math>-1</math> est un carré dans <math>\mathbb{F}_q</math> si et seulement si <math>q \equiv 1 \pmod{4}</math></p> <p><u>Appli 35</u> Théorème des deux carrés      Un entier est somme de deux carrés si et seulement si <math>p \equiv 1 \pmod{4}</math></p> <p><u>Appli 36</u> : Il existe une infinité de nombres premiers de la forme <math>4n+1</math></p> <p><u>Exercice 37</u> l'équation <math>ax^2 + by^2 = 1</math> d'inconnues <math>(x, y) \in K^2</math> avec <math>(a, b) \notin (K^*)^2</math> admet une seule solution sur <math>K</math>.</p> <p><u>Théorème 38</u> Réciprocité quadratique      Soient <math>p, q</math> deux nombres premiers impaires distincts, alors <math>(\frac{p}{q}) (\frac{q}{p}) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}</math></p> <p><u>Application 39</u> Si <math>x^2 = \pi</math> pi arrête pi premier  <math>(\frac{2}{p}) = \pi (\frac{2}{p})</math> donc on peut calculer <math>(\frac{2}{p})</math> en fonction de <math>(\frac{p}{2})</math> pour <math>p \neq 2</math> non premier.</p> <p><u>Exemple 40</u> : <math>(\frac{12}{3}) = (\frac{-1}{3}) = -1</math> donc <math>(\frac{12}{3}) = (\frac{12}{3}) = (-1)^{\frac{12-1}{2} \frac{3-1}{2}} = (-1)^8 = 1</math> donc <math>3</math> est la somme de deux carrés de <math>\mathbb{Z}</math>.</p>

# Dvts possibles

- Algo de Berlekamp  
factorisa<sup>o</sup> de polynomes sur corps finis → permet de factoriser  
sur  $\mathbb{Z}$  ensuite  
PRASOLOV, Polynomials p217
- Théorème de Wederkarn  
ts les corps finis sont commutatifs  
sert ds la démo que corps fini de card  $p^k$  car ds la démo on  
a besoin que  $X^2X$  a au + q  $\sqrt{}$ , veut que ds corps comm.  
( $X^2-1$  a 4  $\sqrt{}$  ds  $\mathbb{Q}$  quaternions) → à mentionner ds le plan.  
utilise les polynomes cyclotomiques.

## Applications des corps finis

- Cryptographie AES / DES  
Codes correcteurs d'erreur (Plan)  
↳ Demazure, cours d'algèbre & Mendry, cours d'arithmétique
- Algorithme  $p \pm 1$  de WILLIAMS
- Gauss-Van der Waerden? (Un peu finitc)  
= construct<sup>o</sup> à la règle et au compas
- Comb corps fini permet de retrouver des phs sur corps  $\Rightarrow$   
 $\text{Chm-} \varphi: \mathbb{C}^n \rightarrow \mathbb{C}^n \text{ poly.}$  Alors  $\varphi$  injective  $\Rightarrow \varphi$  bijective  
 $\uparrow$  (= en ses coord.)  
cf page web Winckler, Bruno.

(Exercices)  $\circ$  : finale

II)  $\text{Isg aut}(\mathbb{F}_q) = \{ \sigma^n, n \in \mathbb{N} \}$

$\mathbb{F}_q = \mathbb{F}_p[X]/P$  avec  $P$  irred. de deg  $n$ .

$\omega$  une r de  $P \Rightarrow \omega^{p^k} \in \mathbb{F}_q \iff 0 \leq k \leq n-1$

On veut n r.

Si  $\omega^{p^k} = \omega$ ,  $\omega^{p^{k-1}} = 1$  de  $\mathbb{F}_q^*$   $\omega$  d'ordre  $|p^{k-1} - 1|$

Donc  $\{ \sigma^k X^{p^k} - X \}$  forme un  $n$ -corps strict de  $\mathbb{F}_q$  qui contient  $\omega$  et  $\mathbb{F}_p$  Absurde car  $\mathbb{F}_q$  corps de rupture de  $P$

Si  $\omega^{p^k} = \omega^{p^l}$ ,  $k < l$ . (on les veut  $\neq b$ )

$$(\omega^{p^k})^{p^{n-k}} = \omega^{p^n} = (\omega^{p^l})^{p^{n-l}} = \omega^{p^l} \omega^{p^{n-l}} = (\omega^{p^l})^{p^{n-l}} = \omega^{p^n} \rightarrow \text{revenir \u00e0 cas pr\u00e9c\u00e9d}$$

Thm base normale.  
 $\mathbb{F}_q = \mathbb{F}_p(\omega, \omega^p, \dots, \omega^{p^{n-1}})$   
 $(1, \omega, \omega^p, \dots, \omega^{p^{n-1}})$   
= base de  $\mathbb{F}_q$

III)  $X^2 - bX + c$  irr\u00e9ductible sur  $\mathbb{F}_p$ ,  $p$  premier.

Isg.  $X^2 - bX + c \mid X^{p^2} + X - b$ .

Soit  $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/X^2 - bX + c$ .

Soit  $\omega$  r de  $X^2 - bX + c$ .

$\omega^p$  est r de  $X^2 - bX + c$  (Frobenius)  $\rightarrow$  on a nos 2 r!

Relat<sup>o</sup> coeff/r:  $\omega + \omega^p = b$  et  $\omega\omega^p = c$

$\omega$  r de  $X^{p^2} + X - b$

$\hookrightarrow \text{Pgcd}(P, X^{p^2} + X - b) \neq 1$

$\hookrightarrow P$  irr\u00e9ductible  $\rightarrow \text{Pgcd} = P : P \mid X^{p^2} + X - b$

IV)

Exercices

de deg 2

$\vec{x} + \vec{x} + \vec{z} \in$  faire le Picking et systéma. nq uemb. regarder.

I) Trouver deux poly irréductibles sr  $\mathbb{F}_3$ .

$$\begin{pmatrix} X-2 \cdot 1+1+2 = 1 \\ X-1 \cdot 1+2+2 = 2 \\ \dots : 2 \end{pmatrix}$$

$$\mathbb{F}_3[X] / X^2+1 = \mathbb{F}_3[X] / X^2+X-1 = \mathbb{F}_9 \text{ (cà isomorphé préré)}$$

Construire isomorph. ( $\varphi$ )

$$\sqrt{\phantom{x}} \text{ de } X^2+1 = \omega_1, \omega_2, \sqrt{\phantom{x}} \text{ de } X^2+X-1 = \gamma_1, \gamma_2$$

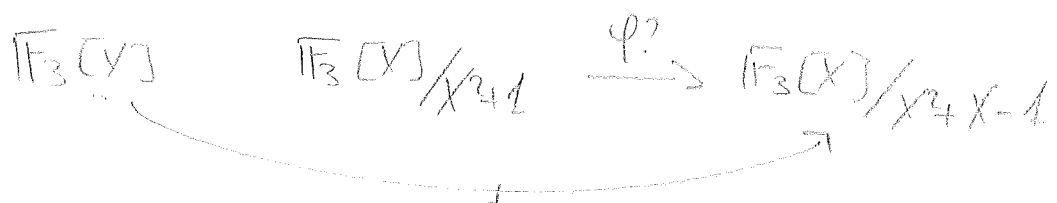
On peut voir  $\mathbb{F}_3[X] / X^2+1$  comme un ev de dim 3 de base  $(1, \omega_1, \omega_2)$

$$\begin{matrix} X^2+X-1 & \dots & \dots & \dots \\ & & & (1, \gamma_1, \gamma_2) \end{matrix}$$

Il faut envoyer la base sr la base et  $\varphi(1) = 1$ .

Donc 2 morph possibles:  $\omega_1 \mapsto \gamma_1$  ou  $\omega_1 \mapsto \gamma_2$

On veut exprimer isomorphé comme  $X \mapsto ?$



On cherche  $\phi$  morph surjectif de noyau  $X^2+1$

$\rightarrow$  permet de quotienter par le noyau et obtenir un isomorphé de  $\mathbb{F}_3[X] / X^2+1 \xrightarrow{\varphi} \mathbb{F}_3[X] / X^2+X-1$

$$\alpha = \bar{X} \text{ ds } \mathbb{F}_3[X] / X^2+1$$

$$\beta = \bar{X} \text{ ds } \mathbb{F}_3[X] / X^2+X-1$$

$$\underbrace{\beta^2 + \beta - 1}_0 = \beta^2 - 2\beta - 1 = (\beta - 1)^2 - 2 \underset{=+1}{}$$

$$\alpha \mapsto \beta - 1$$

$$X \mapsto X-1, \phi(X^2+1) = (X-1)^2 + 1 = X^2 - 2X + 1 + 1 = 0 \in \text{Ker } \phi$$

On peut quotienter par  $X^2+1 \subset \text{Ker } \phi$ .

2 méthodes: - montrer que  $X^2+1 = \text{Ker } \phi$  (ici) (prop 4)

- isomorphé de corps = nxl ou injectif

(car morphé de corps = morphé d'anneau  $\Rightarrow$ )

Ker = idéal. Ds un corps  $\Rightarrow$  Ker =  $\{0\}$  ou corps

[  $a \in I \Rightarrow \forall b \in A, ab \in I$ , corps:  $\exists a \in I \setminus \{0\} \Rightarrow a^{-1} \cdot 1 \in I \Rightarrow I = A$  ]

Reciprocité quadratique : peut se dem. de bcp de manière

- thm de Frobenius-Zolotarev

$u \in \mathbb{F}_p^\times$ , signature  $\chi = \left(\frac{du}{p}\right)$ ,  $\chi$  ev sur  $\mathbb{F}_p$   
appliqué à l'automorphisme de Frobenius  
& objectif agrégation

↳ bcp de dems possible  
(cf. Lemmermeyer, Reciprocity...)

## Loi de réciprocité quadratique par les formes quadratiques

**Lemme.** Soient  $a$  un entier non nul et  $q$  un nombre premier impair. Alors

$$|\{x \in \mathbb{F}_q, ax^2 = 1\}| = 1 + \left(\frac{a}{q}\right).$$

**Démonstration :** comme  $a$  est un carré modulo  $q$  si et seulement si  $a^{-1}$  en est un, il est équivalent de dire que  $a$  est un carré modulo  $q$  et que le polynôme  $aX^2 - 1 \in \mathbb{F}_q[X]$  possède deux racines distinctes dans  $\mathbb{F}_q$ . Ainsi, le cardinal considéré vaut 0 si  $a$  n'est pas un carré modulo  $q$ , et 2 si  $a$  est un carré modulo  $q$ . Comme on peut encore écrire, de façon atrocement astucieuse,  $0 = 1 - 1$  et  $2 = 1 + 1$ , le résultat suit. ■

**Théorème.** Soient  $p$  et  $q$  deux nombres premiers impairs. On a

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

**Démonstration :** considérons l'ensemble

$$X = \left\{ (x_1, \dots, x_p) \in \mathbb{F}_q^p, \sum_{i=1}^p x_i^2 = 1 \right\}.$$

On va calculer son cardinal modulo  $p$  de deux façons différentes.

Tout d'abord, on peut le voir comme

$$X = \{x \in \mathbb{F}_q^p, f(x) = 1\},$$

où  $f$  est la forme quadratique dont la matrice dans la base canonique de  $\mathbb{F}_q^p$  est  $I_p$ . Posons

$$d = \frac{p-1}{2}, a = (-1)^d \text{ et } J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{F}_q),$$

et considérons la forme quadratique dont la matrice dans la base canonique de  $\mathbb{F}_q^p$  est

$$M = \begin{pmatrix} J & & & \\ & \ddots & & \\ & & J & \\ & & & a \end{pmatrix} \in \mathcal{M}_p(\mathbb{F}_q).$$

On constate que  $\text{rg}(M) = p = \text{rg}(I_p)$  et  $\det M = (\det J)^d a = (-1)^d (-1)^d = 1 = \det I_p$ . D'après la classification des formes quadratiques sur les corps finis,  $M$  et  $I_p$  ayant même rang et même déterminant (donc même discriminant, qui est le déterminant modulo les carrés du corps de base), elles sont congruentes. Ainsi  $|X| = |X'|$ , où

$$X' = \{x \in \mathbb{F}_q^p, f'(x) = 1\},$$

et  $f'$  est la forme quadratique dont la matrice dans la base canonique de  $\mathbb{F}_q^p$  est  $M$ ; autrement dit, on a

$$X' = \left\{ (y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^p, 2 \sum_{i=1}^d y_i z_i + at^2 = 1 \right\}.$$

Il suffit donc de déterminer le cardinal de  $X'$ . Soit  $(y_1, z_1, \dots, y_d, z_d, t) \in X'$ .

- si  $y_1 = \dots = y_d = 0$ , alors le choix des  $z_i$  est quelconque, et  $t$  doit vérifier  $at^2 = 1$ . Ainsi, il y a  $q^d$  choix des  $z_i$  et  $1 + \left(\frac{a}{q}\right)$  choix de  $t$  d'après le lemme. Il y a donc  $q^d \left[1 + \left(\frac{a}{q}\right)\right]$  éléments de cette forme;
- au contraire, s'il existe un  $y_i$  non nul, alors  $(y_1, \dots, y_d)$  est un vecteur non nul de  $\mathbb{F}_q^d$ , pour lequel il y a  $q^d - 1$  choix. Le choix de  $t$  est quelconque, et alors les  $z_i$  vivent dans un hyperplan affine de  $\mathbb{F}_q^d$ , il y a donc  $q^{d-1}$  choix pour eux. Au total, il y a  $(q^d - 1)qq^{d-1} = q^d(q^d - 1)$  éléments de cette forme

Par suite,

$$|X'| = q^d \left[ 1 + \left(\frac{a}{q}\right) + q^d - 1 \right] = q^d \left( \left(\frac{a}{q}\right) + q^d \right).$$

À présent, on fait agir  $\mathbb{Z}/p\mathbb{Z}$  sur  $X$  par  $k \cdot (x_1, \dots, x_p) = (x_{k+1}, \dots, x_{k+p})$ , les indices étant vus modulo  $p$ . Il y a deux sortes d'orbites :

- celles dont le stabilisateur est  $\mathbb{Z}/p\mathbb{Z}$ , elles sont de la forme  $\{(x, \dots, x)\}$ , où  $x \in \mathbb{F}_q$  vérifie  $f(x, \dots, x) = 1$ , c'est-à-dire  $px^2 = 1$ ;
- les autres, dont le stabilisateur, étant un sous-groupe de  $\mathbb{Z}/p\mathbb{Z}$ , est forcément trivial.

L'équation aux classes nous donne alors

$$|X| = \sum_{px^2=1} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\mathbb{Z}/p\mathbb{Z}|} + \sum_{\text{autres orbites}} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\{1\}|} \equiv 1 + \left(\frac{p}{q}\right) [p]$$

grâce au lemme.

On en conclut que

$$q^d \left( \left(\frac{a}{q}\right) + q^d \right) \equiv 1 + \left(\frac{p}{q}\right) [p].$$

Comme  $q^d \equiv \left(\frac{q}{p}\right) [p]$  et que de même  $\left(\frac{a}{q}\right) \equiv (-1)^{\frac{p-1}{2} \frac{q-1}{2}} [p]$ , on obtient en multipliant cette identité par  $\left(\frac{q}{p}\right)$

$$(-1)^{\frac{p-1}{2} \frac{q-1}{2}} + \left(\frac{q}{p}\right) \equiv \left(\frac{q}{p}\right) + \left(\frac{q}{p}\right) \left(\frac{p}{q}\right) [p].$$

Simplifiant par  $\left(\frac{q}{p}\right)$ , on obtient le résultat voulu modulo  $p$ . Mais comme chaque membre est un entier égal à  $\pm 1$ , c'est en fait une égalité dans  $\mathbb{Z}$ . ■

Dev 2  
2/2