(123)

(123) 1/2

NOM : SERAPHIN Prénom : Carine Jury :

(Algèbre) – Entourez l'épreuve → Analyse

Sujet choisi : 123 Corps finis. Applications

Autre sujet :

DEV 1

(123) (123) 2/2

NOM : SERAPHIM Prénom : Carim Jury :

(Algèbre) – Entourez l'épreuve → Analyse

Sujet choisi : 123 corps finis. Application

Autre sujet :

| Dvlts possibles |

- Algo de Berlekamp
  factorisa° de polynomes s/ corps finis → permet de factoriser s/ Z ensuite
  PRASOLOV, Polynomials p217
- Théorème de Wederburn
  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 $X^q - X$ a au + q $\sqrt{}$, vrai que ds corps comm.
  ($X^2 - 1$ a 4 $\sqrt{}$ ds les quaternions) → à mentionner ds le plan.
  utilise les polynomes cyclotomiques

| Applications des corps finis |

- Cryptographie AES / DES
  Codes correcteurs d'erreur
  ↳ Demazure, cours d'algèbre & Hendry (Flore), cours d'arithmétique
- Algorithme p+1 de WILLIAMS
- Gauss-Wantzel ? (Un peu limite)
  = construc° à la règle et au compas
- Cmt corps fini permet de résoudre des pbs s/ corps →
  Thm $\varphi : \mathbb{C}^n \to \mathbb{C}^n$ poly. Alors φ injective ⇒ φ bijective
  ↖ (= en ses coord.)
  c/ page Web Winckler, bruno.

| Exercices | ⊃ : facile

(II) Mq $\mathrm{aut}(\mathbb{F}_q) = \{Fr^n,\ n \in \mathbb{N}\}$ $q = p^n$

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

ω une racine de P ⇒ ω^{p^k} racine ? $0 \leq k \leq n-1$

On veut n racines.

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

Donc $\{$racines $X^{p^k} - X\}$ forme un ss-corps strict de $\mathbb{F}_q$ qui contient ω et $\mathbb{F}_p$. Absurde car $\mathbb{F}_q$ corps de rupture de P

Si $\omega^{p^k} = \omega^{p^\ell}$, $\ell < k$. (on les veut ≠)

$(\omega^{p^k})^{p^{n-k}} = \underset{\omega}{\omega^{p^n}} = (\omega^{p^\ell})^{p^{n-k}} = \omega^{p^\ell} \times \omega^{p^{n-k}} = \underset{\omega}{(\omega^n)}^{p^{\ell-k}} = \omega^{p^{\ell-k+n}}$ → ramené au cas préc.

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

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

Mq. $(X^2 - bX + c) \mid X^p + X - b$.

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

Soit ω racine de $X^2 - bX + c$.

ω^p est racine de $X^2 - bX + c$ (Frobenius) } → on a nos 2 racines !

Rela° coeff/racines : $\omega + \omega^p = b$ et $\omega\omega^p = c$

⇓

ω racine de $X^p + X - b$

↳ Pgcd $(P, X^p + X - b) \neq 1$

+ P irréductible → Pgcd = P : $P \mid X^p + X - b$

(IV)

[Exercices]

I) Trouver deux poly irréductibles (de deg 2) sur $\mathbb{F}_3$.

$X^2 + 2X + 2$ ← faire le listing et systématiquement regarder.

$X = 2 : 1 + 1 + 2 = 1$
$X = 1 : 1 + 2 + 2 = 2$
$X = 0 : 2$

X^2+1 & X^2+X-1.

$\mathbb{F}_3[X]/X^2+1 = \mathbb{F}_3[X]/X^2+X-1 = \mathbb{F}_9$ (à isomorphisme près)

Construire l'isomorφ. (φ)

$\sqrt{}$ de $X^2+1 = \omega_1, \omega_2$. $\sqrt{}$ 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 $(1, \omega_1, \omega_2)$

———— $/X^2+X-1$ ———— $(1, \gamma_1, \gamma_2)$.

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

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

On veut exprimer l'isomorφ comme $X \mapsto$?

$$\mathbb{F}_3[X] \qquad \mathbb{F}_3[X]/X^2+1 \xrightarrow{\varphi ?} \mathbb{F}_3[X]/X^2+X-1$$

(flèche ϕ de $\mathbb{F}_3[X]$ vers $\mathbb{F}_3[X]/X^2+X-1$)

On cherche ϕ morφ surjectif de noyau X^2+1
→ permet de quotienter par le noyau et obtenir un isomorφ de
$\mathbb{F}_3/X^2+1 \xrightarrow{\varphi} \mathbb{F}_3[X]/X^2+X-1$

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

$\underbrace{\beta^2+\beta-1}_{=0} = \beta^2 - 2\beta - 1 = (\beta-1)^2 \underbrace{-2}_{=+1}$

$\alpha \mapsto \beta - 1$

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

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

2 méthodes : – montrer que $X^2+1 = \text{Ker}\,\phi$
– φ morφ de corps = nul ou injectif (ici) (prop 4)
(car morφ de corps = morφ d'anneau ⇒ Ker = idéal. Ds un corps ⇒ Ker = {0} ou corps)

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

Réciprocité quadratique : peut se dem. de bcp de manière

- Thm de Frobenius-Zolotarev
  $u \in GL(V)$ signature $u = \left(\frac{\det u}{p}\right)$, V ev sur $\mathbb{F}_p$
  appliqué à l'automorphe de Frobenius
  & Objectif aujourd'hui

Caldero Histoire hédoniste de gpe et de geom p183 (123)

→ bcp de dem 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*

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

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

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

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

Tout d'abord, on peut le voir comme

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

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

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

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

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

Dev 2
1/2

On constate que $\mathrm{rg}(M) = p = \mathrm{rg}(I_p)$ 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

$$X' = \left\{x \in F_q^p, f'(x) = 1\right\},$$

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

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

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

- si $y_1 = \ldots = y_d = 0$, 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 $(y_1, \ldots, y_d)$ 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 $k \cdot (x_1, \ldots, x_p) = (x_{k+1}, \ldots, x_{k+p})$, 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 $\{(x, \ldots, x)\}$, où $x \in \mathbb{F}_q$ vérifie $f(x, \ldots, x) = 1$, 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 ± 1, c'est en fait une égalité dans $\mathbb{Z}$. ■