NOM : MAURAS Prénom : Simon Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : 123 Corps finis. Applications

Autre sujet :

Perrin, Beck, Gourdon

Les corps seront supposés commutatifs à l'exception du théorème 15. On suppose connues les notions de base sur les anneaux, les corps et les espaces vectoriels.

I Corps et Polynômes

Def 1 (Extension de corps) Soit $K \subseteq L$ des corps. L est une extension (de corps) de K.

Def 2 (Degré d'une extension) Soit L une extension de K. L est un K-espace vectoriel et on note $[L:K] = \dim_K L$.

Thm 3 (Base télescopique) Soit $K \subseteq L \subseteq M$ des corps. $(e_i)_I$ une base de L sur K. $(f_j)_J$ une base de M sur L. Alors $(e_i f_j)_{I \times J}$ est une base de M sur K.

Def 4 (Espaces engendrés) Soit $K \subseteq L$ des corps et $A \subseteq L$

- $K[A]$ est le plus petit anneau contenant K et A.
- $K(A)$ est le plus petit corps contenant K et A.
- $K[X]$ est l'anneau des polynômes à coefficients dans K.

Def 5 (Transcendant / Algébrique) Soit $K \subseteq L$ et $\alpha \in L$. Il existe un unique $\varphi : K[X] \to L$ tel que $\varphi_{|K} = id$ et $\varphi(X) = \alpha$. Si φ est injectif, α est transcendant. Sinon α est algébrique.

Prop 6 (Caractérisation algébrique) Soit $K \subseteq L$ et $\alpha \in L$ (α algébrique sur K) $\iff$ $(K(\alpha) = K[\alpha]) \iff ([K(\alpha):K] < +\infty)$

Def 7 (Algébriquement clos) Un corps K est algébriquement clos si pour toute extension L, tout $\alpha \in L$ est algébrique sur K.

Ex 8 (Théorème d'Alembert-Gauss) $\mathbb{C}$ algébriquement clos

Def 9 (Corps de rupture) Soit K corps et $P \in K[X]$ irréductible. Un corps de rupture de P est une extension $K(\alpha)$ avec $P(\alpha) = 0$.

Thm 10 (Existence et Unicité du corps de rupture) Soit K corps et $P \in K[X]$ irréductible. $K[X]/(P)$ est l'unique corps de rupture de P à isomorphisme près

Def 11 (Corps de décomposition) Soit K corps et $P \in K[X]$. Un corps de décomposition est une extension $K \subseteq L$ minimale telle que P est produit de facteurs de degré 1 dans $L[X]$.

Thm 12 (Existence et Unicité du corps de décomposition) Soit K corps et $P \in K[X]$. On note $D_K(P)$ l'unique corps de décomposition de P à isomorphisme près.

Def 13 (Clôture algébrique) Une extension $K \subseteq \overline{K}$ est une clôture algébrique si $\overline{K}$ est algébriquement clos et que tout élément $\alpha \in \overline{K}$ est algébrique sur K.

Application 14 (Polynômes cyclotomiques) Soit K corps. On note $P_n(X) = X^n - 1$ et $K_n = D_K(P_n)$ son corps de décomposition. Une racine $n$ième primitive est un élément $\zeta \in K_n$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour $d < n$. On note μ_n^* l'ensemble des racines n-ième primitives.

$$\Phi_n(X) := \prod_{\zeta \in \mu_n^*} (X - \zeta) \qquad \text{($n$ième polynôme cyclotomique)}$$

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X) \qquad \text{(décomposition effective)}$$

Thm 15 (Wedderburn) Tout corps gauche (non supposé commutatif) de cardinal fini est commutatif.

II Corps finis

Prop 16 L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier

Def 17 (Sous corps premier) Le sous corps premier d'un corps K est le plus petit sous corps contenant 1.

123 Corps finis. Applications

Def 18 (Caractéristique) Soit K un corps et $\varphi : \mathbb{Z} \to K$ tel que $\varphi(n) = \underbrace{1 + \dots + 1}$. φ est un morphisme et $\mathrm{Ker}\,\varphi = p\mathbb{Z}$ avec p premier ou nul. On note car $K = p$.

Prop 19 (Cardinal et caractéristique) Soit K un corps
- Si car $K = 0$, K est infini, son sous corps premier est $\mathbb{Q}$
- Si $|K| < \infty$, car $K = p > 0$, son sous corps premier est $\mathbb{Z}/p\mathbb{Z}$. De plus $n = [K : \mathbb{Z}/p\mathbb{Z}] < +\infty$ et $|K| = p^n$

Prop 20 (Homomorphisme de Frobenius) Soit K de caractéristique $p > 0$. On pose $F : \begin{cases} K \to K \\ x \mapsto x^p \end{cases}$ l'homomorphisme de Frobenius
- Si K est fini, F est bijectif
- Si K est $\mathbb{Z}/p\mathbb{Z}$, $F = \mathrm{Id}_K$

Thm 21 (Existence et unicité des corps finis) Soit p un nombre premier et n dans $\mathbb{N}^*$. On pose $q = p^n$. $D_{\mathbb{Z}/p\mathbb{Z}}(X^q - X)$ est l'unique corps à q éléments à un isomorphisme près. On le note $\mathbb{F}_q$.

Thm 22 (Groupe $(\mathbb{F}_q^*, \times)$) Le groupe $\mathbb{F}_q^*$ est cyclique.

Prop 23 (Dénombrage de $\mathbb{F}_q^*$) On a une suite exacte

$$1 \to \mathbb{F}_q^{*2} \to \mathbb{F}_q^* \to \{-1, 1\} \to 1$$
$$x \longmapsto x^{\frac{q-1}{2}}$$

En particulier $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$

III Application : Polynômes irréductibles

Prop 24 (Quotient par un idéal maximal) Soit A un anneau. Le quotient A/I est un corps ssi I est un idéal maximal

Prop 25 (Construction alternative d'un corps fini) Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Si $P \in \mathbb{F}_p[X]$ est un polynôme irréductible de degré n, alors $\mathbb{F}_p[X]/\langle P \rangle$ est un corps de cardinal p^n.

Prop 26 (Critère d'Eisenstein) Soit A un anneau factoriel et K son corps des fractions rationnelles. Soit $p \in A$ irréductible. Soit $P(X) = \sum_{i=0}^{m} a_i X^i$ dans $A[X]$ tel que $p \nmid a_m$, $\forall 0 \leq i < m$ $p \mid a_i$ et $p^2 \nmid a_0$. Alors P est irréductible dans $K[X]$.

Ex 27 $X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Z}$

Prop 28 (Irréductibilité et réduction) Soit A un anneau factoriel et K son corps des fractions. Soit I un idéal premier de A et $B = A/I$ qui est un anneau intègre, de corps de fractions L.
Soit $P(X) = \sum_{i=0}^{m} a_i X^i$ dans $A[X]$ et $\overline{P}$ sa réduction modulo I.
Si $\overline{P}$ irréductible sur B (ou L) et $\overline{a}_m \neq 0$ alors P irréductible sur K

Ex 28 $X^3 + 462X^2 + 2433X - 67691$ irréductible sur $\mathbb{Z}$.

Prop 29 (Irréductibilité et extension) Soit $P \in K[X]$ de degré n. P irréductible sur K ssi P n'a pas de racine dans toute extension $K \subseteq L$ vérifiant $[L : K] \leq n/2$

Ex 30 $X^4 + X + 1$ irréductible sur $\mathbb{F}_2$ donc $3X^4 + 12X^2 - 7X + 9$ est irréductible sur $\mathbb{Z}$.

Remarque 31 Réciproque à 28 fausse : $X^4 + 1$ est irréductible sur $\mathbb{Z}$ (et $\mathbb{Q}$) mais réductible sur $\mathbb{F}_p$ pour tout p.

Prop 32 (Conservation de l'irréductibilité par extension de corps) Soit $P \in K[X]$ irréductible de degré n. Soit $K \subseteq L$ une extension telle que $\mathrm{pgcd}(n, [L : K]) = 1$. Alors P irréductible dans L.

Ex 33 $X^3 + X + 1$ irréductible dans $\mathbb{F}_{2^n}$ avec $n \not\equiv 0 \, [3]$

Prop 34 (Élévation à la puissance q) Soit $R \in \mathbb{F}_q[X]$

$$S_R : \begin{cases} \mathbb{F}_q[X]/(R) \to \mathbb{F}_q[X]/(R) \\ Q(X) \bmod R \mapsto Q(X^q) \bmod R \end{cases}$$

Pour tout Q, $S_R(Q) = Q^q$

Prop 35 Soit $P \in \mathbb{F}_q[X]$ et V un vecteur propre de S_P associé à la valeur propre 1 (dans $\mathrm{Ker}(S_P - \mathrm{Id})$).

Alors $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V-\alpha)$

<u>Thm 36</u> (Algorithme de Berlekamp) Soit $P \in \mathbb{F}_p[X]$

- Si P constant, P irréductible
- Si $\mathrm{pgcd}(P,P')=0$, alors $P'=0$ donc $\exists R$, $R^p = P$
  Recommencer avec R.
- Si $\mathrm{pgcd}(P,P') = Q$, avec $Q \notin \{0,1\}$
  Recommencer avec Q et P/Q
- Si $\mathrm{pgcd}(P,P') = 1$, il n'y a pas de racines doubles
  Si $\dim(\mathrm{Ker}\, S_p - Id) = 1$ P irréductible
  Sinon soit V une valeur propre de degré ≥ 1.
  Recommencer avec les $\{\mathrm{pgcd}(P, V-\alpha) \mid \alpha \in \mathbb{F}_p\}$

<u>Ex 37</u> Montrer que $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$

IV Application : Codes correcteurs

<u>Rem 38</u> $\mathbb{F}_q^n$ est un $\mathbb{F}_q$ espace vectoriel

<u>Def 39</u> (Codes) Code correcteur : sous ensemble de $\mathbb{F}_q^n$
Code linéaire : sous e.v. de $\mathbb{F}_q^n$
Code cyclique : code linéaire stable par décalage.

<u>Def 40</u> (Matrice génératrice)
Soit C un code linéaire de taille n et de dimension m.
Il existe une matrice G telle que $C = \mathrm{Im}\, G = \{Gx \mid x \in \mathbb{F}_q^m\}$

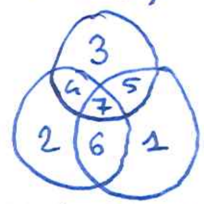
<u>Def 41</u> (Distance de Hamming) Soit C un code correcteur et $x, y \in C$. Le poids de Hamming $\omega(x)$ est le nombre de coefficients non nuls. La distance de Hamming est $d(x,y) = \omega(x-y)$

<u>Def 42</u> (Distance minimale) Soit C un code correcteur
$d = \min\{d(x,y) \mid x \neq y\}$
Si C est linéaire $d = \min\{\omega(x) \mid x \neq 0\}$

<u>Prop 43</u> (Borne Singleton) Soit C un code linéaire
$d \leq n+1-m$ ou $|C| \leq q^{n-d+1}$

<u>Prop 44</u> (Borne de Hamming) Soit C un code correcteur
$$|C| \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i} \quad \text{avec } t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

<u>Ex 45</u> (Code de Hamming 7-4-3)
$$G = \begin{pmatrix} 0&1&1&1 \\ 1&0&1&1 \\ 1&1&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix}$$



Calcul de $|C|$, d, comment encrypter / décrypter ?