Corps finis

Wedderburn : Tout corps fini et commutatif .

Exemples 1) $\mathbb{Z}/p\mathbb{Z}$ avec p premier

2) $\mathbb{Z}/p\mathbb{Z}[X] / (P)$ avec p premier et P polynôme irréductible

Caractéristiques d'un anneau

Définition: La caractéristique de A est le plus petit entier naturel $n\neq 0$ pour lequel $1_A(n\mathbb{Z})=0$ (exemple 5 pour $\mathbb{Z}/5Z$)

■ Soit K un corps d'élément neutre 1k, de caractéristique c(K), et m ∈K.

→ Si n n'existe pas c(K) =0 on a m1k = 0 si et seulement si m=0 et K contient un sous-espace isomorphe à $\mathbb{Q}$.

→ Si c(K) = p (premier) on a m1k=0 si et seulement si p divise m et K contient un sous-espace isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

C'est le cas de tout corps fini: on a c(K)=p et il existe une entier n≥ 1 tel que card(K) = p^n.

Un corps fini de cardinal p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exemples: avec p premier $c(\mathbb{Z}/p\mathbb{Z})=p$, $card(\mathbb{Z}/p\mathbb{Z}) =p$ et si P irréductible de degré n $c(\mathbb{Z}/p\mathbb{Z}[X]/(P)) = p$, $card(\mathbb{Z}/p\mathbb{Z}[X]/(P)) =p^n$

Groupe multiplicatif d'un corps fini

■ **Soit K un corps commutatif et H sous-groupe fini de K¤ (éléments inversibles) , alors H est cyclique.**
Si K est un corps fini, K¤ est cyclique.

La démonstration s'appuie sur

soit G, groupe multiplicatif commutatif . Dans G x est d'ordre n, y d'ordre m (n,m premiers entre eux) alors xy est d'ordre mn

Si G est fini, x∈G, y∈G, x d'ordre n et y d'ordre m, il existe dans G un élément z d'ordre PPCM(m,n).

■ **K corps fini de cardinal p. k¤ possède exactement φ(p-1) générateurs (φ indicatrice d'Euler) .**
Si α est l'un des générateurs on peut tous les exprimer sous la forme α^k avec 1≤ k≤ p-1 et k premier avec p-1.

$K=\mathbb{Z}/2\mathbb{Z}[X]/(X^4+X+1)$ est un corps de caractéristique 2 et contenant 2^4 = 16 éléments.

K¤ contient φ(15) éléments qui peuvent s'écrire α^k avec α générateur et k ∈{1,2,4,7,8,11,13,14}

Les coefficients des polynômes de K sont 0 ou 1, leur degré ≤ 3. et $x^4 +x \equiv 1$. x est inversible puisque $x(x^3+1)\equiv 1$

On a

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^k	x	x^2	x^3	$x+1$	x^2+x	x^3+x^2	x^3+x+1	x^2+1	x^3+x	x^2+x+1	x^3+x^2+x	x^3+x^2+x+1	x^3+x^2+1	x^3+1

Comme $x^{15} \equiv 1$, l'inverse de x^k est x^{15-k}. Par exemple $(x+1)(x^3+x^2+x) = x^4+2x^3+2x^2+x \equiv x^4+x \equiv 1$ (Dans $\mathbb{Z}/2\mathbb{Z}$ on a $2 \equiv 0$)

Corps finis de la forme $\mathbb{Z}/p\mathbb{Z}[X] / (P)$

■ **Si K est un corps card(K)= p^n,**
il existe un polynôme P irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ tels que K soit isomorphe à $\mathbb{Z}/p\mathbb{Z}[X]/(P)$.

Construction et unicité des corps à p^2 éléments

■ **Tous les corps de cardinal p^2 (p premier) sont isomorphes.**

Pour p=2 le seul polynôme de degré 2 irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$ est x^2+x+1 puisque $x^2+x=x(x+1)$ et $x^2+1 =(x+1)^2$.

Si p impair il y a p^2 polynômes unitaires de degré2. p s'écrivent $(x-a)^2$ et p(p-1)/2 s'écrivent (x-a)(x-b)→ p(p–1)/2 irréductibles.

Il existe donc des corps à p^2 éléments. Ensuite il faut démontrer que si K isomorphe à $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ et K' à $\mathbb{Z}/p\mathbb{Z}[X]/(Q)$, Pet Q étant irréductibles de degré 2, K et K' sont isomorphes. Or $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ et $\mathbb{Z}/p\mathbb{Z}[X]/(Q)$ étant formé des mêmes p^2 polynômes de degré 1 identiques, on a des isomorphismes entre K ↔ $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ ↔ $\mathbb{Z}/p\mathbb{Z}[X]/(Q)$ ↔K' et donc entre K et K'.

Polynômes irréductibles sur un corps fini

Si K est un corps fini de caractéristique p et de cardinal q = p^n

■ pour tout x,y∈K et tout entier naturel n on a $(x+y)^{p^n} = x^{p^n} + y^{p^n}$

■ Soit L corps fini contenant K, **x élément de L x ∈K si et seulement si x^q = x**

P élément de L[X], P∈K[X] si et seulement si $P(X^q)=[P(X)]^q$.

Si P irréductible dans K[X] a une racine α dans L, il existe un plus petit entier r tel que $\alpha^{q^r} = \alpha$.

r est le degré de P et P=$\prod_{d=0}^{d=r-1}(x-\alpha^{q^d})$. P a toutes ses racines dans L, ce sont les α^{q^d}, avec 0 ≤ d ≤ r-1.

■ Soit K de cardinal q et n un entier naturel non nul.

Les diviseurs irréductibles de $X^{q^n} - X$ ∈ K[X] sont tous ceux dont le degré divise n.

$X^{q^n} - X$ =$\prod P_i$ ou Pi parcourt l'ensemble des polynômes irréductibles de K[X] dont le degré divise n.

Théorème d'existence et dénombrement

Card(K)=q , $I_m(q)$ est le nombre de polynômes irréductibles de degré m≥ 1 de K[X]. Dn = ensemble des diviseurs de n .
Pour tout n ≥ 1 $I_n(q) >0$ $q^n=\sum_{d\in D} dI_d(q)$ pour tout nombre premier p il existe un corps tel que card(K)= p^n.
$nI_n(q)=\sum_{d\in D} \mu(d)\, q^{\frac{n}{d}}$ où **$\mu(d) = (-1)^r$** si d est le produit de r nombre premiers distincts, **= 0** si d divisible par un carré.

Théorème d'unicité

- 2 corps finis ayant le même nombre d'éléments sont isomorphes.