

# Leçon 123 : Corps finis. Applications.

## 1 Corps finis (Perrin, Rombaldi)

### 1.1 Caractéristique

- Définition caractéristique + propriété
- Cardinal possibles pour un corps
- Frobenius

### 1.2 Existence et unicité

- Théorème d'existence/unicité
- Dév 1 : Décomposition de  $P_n = X^{p^n} - X$  + cardinal des polynômes irréductibles
- $\mathbb{F}_q$  c'est aussi  $\mathbb{F}_p/(P_n)$
- Exemple

### 1.3 Sous-structure

- Propriété sur les sous-corps de corps fini
- Groupe des inversibles
- Sous-groupe additifs

## 2 Étude des carrés (Perrin, Rombaldi)

### 2.1 Étude en soi

- Introduction des notations du Perrin

- Cardinal de  $\mathbb{F}_q^2$  et  $\mathbb{F}_q^{*2}$
- Caractérisation des carrés
- $-1$  carré dans  $\mathbb{F}_q$  ssi  $q \equiv 1[4]$

### 2.2 Utilisation des résultats précédents

- Application pour équations diophantiennes
- Définition résidu quadratique + symbole de Legendre
- Une ou deux propriétés de base sur le symbole de Legendre
- Loi de réciprocité quadratique

## 3 Polynômes dans les corps finis (Perrin)

- Rappel que  $\mathbb{K}[X]$  principal
- Quelques remarques du Perrin au choix
- Critère Eisenstein
- Un théorème de réduction + Application
- Dév 2 : Berlekamp

## 4 Dénombrement en algèbre linéaire sur les corps finis (Perrin)

- Centre de  $GL(E)$  et  $SL(E)$
- Définition de  $PGL$  et  $PSL$
- Cardinaux  $GL_n(\mathbb{F}_q)$ ,  $SL_n(\mathbb{F}_q)$  etc.
- Nombre de matrices diagonalisables dans  $\mathcal{M}_n(\mathbb{F}_q)$