112

Corps finis. Appl

I) Structure

1) Caract, ss corps 1er et card

- La caract d'un corps fini est un nbre 1er
  → Si k est un corps fini de caract p (1er), son ss corps 1er est iso à $\mathbb{F}_p$, son card est p^n avec $n = [k : \mathbb{F}_p]$ et $x \mapsto x^p$ est un auto de k (Frobenius)

2) Commutativité

- Th de Wedderburn

3) gpe mult

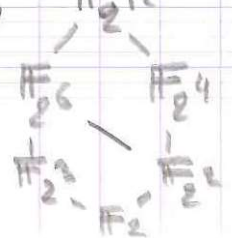
- Le gpe mult d'un corps fini est cyclique
  ⇒ Th de l'élément prim

Dorénavant, p est 1er et $q = p^n$ avec $n \in \mathbb{N}^*$.

II) Existence et unicité

- ∃ corps à q él^{ts} unique à iso près noté $\mathbb{F}_q$. C'est le corps de déc de $X^q - X$ sur $\mathbb{F}_p$.
- Ds $\overline{\mathbb{F}_p}$, $\mathbb{F}_q$ est vraiment unique. C'est {racines de $X^q - X$}
  ⇒ Ds $\overline{\mathbb{F}_p}$, les ss. corps de $\mathbb{F}_q$ st les $\mathbb{F}_{p^d}$ avec $d \mid n$.

Exple : Ds $\overline{\mathbb{F}_2}$,



III) Carrés

1) Cardinal

- Si $p=2$, $\mathbb{F}_q^2 = \mathbb{F}_q$.
  Si $p>2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$
  $\Rightarrow$ classif des f_q sur $\mathbb{F}_q$ avec $p>2$

2) Caract ($p>2$)

- $x \in \mathbb{F}_q^{*2}$ ssi $x^{\frac{q-1}{2}} = 1$
  $\rightarrow -1 \in \mathbb{F}_q^2$ ssi $q \equiv 1 \pmod 4$
  $\Rightarrow$ $\exists$ infté de nbres 1ers de la forme $4n+1$.

3) Symboles de Legendre

Déf: symbole de Legendre
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- loi de réciprocité quad
  $\Rightarrow$ $\exists$ infté de nbres 1ers de la forme $6n+1$

IV) Autour de l'irréd des polyn.

- Th de réd mod p
  $\Rightarrow X^p - X - 1$ est irréd ds $\mathbb{Z}[X]$
- Un polyn de $k[X]$ de deg $n>0$ est irréd ds $k[X]$ ssi il n'a pas de racine ds les ext de k de deg $\leq \frac{n}{2}$
  $\Rightarrow X^4+X+1$ est irréd ds $\mathbb{F}_2[X]$
  $\Rightarrow X^4+1$ est réd ds $\mathbb{F}_p[X]$ pour tt p 1er