112 – Corps finis. A.

« Là, on fait pas dans la dentelle. »

Un petit commentaire avant de commencer : C'est une leçon divine.

Le plan :

I) Structure des corps finis.

1) Généralités.

Corps premier. Caractéristique d'un anneau. Cas des corps. Cas des corps finis. Non existence d'un corps de cardinal 6. Conséquence sur le cardinal d'un corps fini. Morphisme de Frobenius.

2) Corps de rupture et décomposition.

Extension de corps, corps de rupture. Propriété d'unicité à isomorphisme près. Exemple : construction d'un corps à 8 éléments. Corps de décomposition.

3) Existence et unicité des corps finis.

Existence. Unicité à iso près. Notation $\mathbb{F}_q$. Théorème de Wedderburn.

II) Polynômes et $\mathbb{F}_q[X]$.

1) Groupe multiplicatif.

Indicatrice d'Euler. Formule de sommation. Groupe multiplicatif est un groupe cyclique.

2) Irréductibilité.

Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$. Critère de réduction modulo p. Exemple. Remarque sur le degré d'une extension. Contre exemple à la réciproque du critère de réduction modulo p.

3) Construction des corps finis.

Décomposition du polynôme cyclotomique. Formule de factorisation de $X^{p\hat{}n}-X$. Cas des extensions cyclotomiques sur $\mathbb{F}_q$. Construction de $\mathbb{F}_{16}$.

III) Groupe multiplicatif $\mathbb{F}_q^*$.

Les carrés : définitions. Autant de carrés que de non carrés dans $\mathbb{F}_q$ pour $q\neq 2$. $x^{(p-1)/2}=1$ si x est un carré. Corollaire sur la congruence de q modulo 4 selon que -1 soit un carré modulo q ou non. Symbole de Legendre. Homomorphisme de groupe non constant. Sommes de Gauss. Loi de réciprocité quadratique. Exemple. Frobenius-Zolotarev.

IV) Espace vectoriel $\mathbb{F}_q$.

1) Isomorphismes exceptionnels.

Combinatoire algébrique, isomorphismes exceptionnels.

2) Formes quadratiques sur $\mathbb{F}_q$.

Discriminant d'une forme quadratique et classification. Remarque sur la parité de la dimension. Isomorphisme exceptionnel concernant $SO(\mathbb{F}_q)$.

Les développements :

A3 : Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$
A16 : Frobenius-Zolotarev
A25 : Théorème de Wedderburn

La bibliographie :

[Dmz]-[Per]-[FG0]-[BMP]-[Goz]