

112: CORPS FINIS – App

0. Préliminaires [Pe]

1. Polynômes cyclotomiques
def, $X^n - 1 =$
2. Extensions de corps
def-prop : corps de rupture/décomposition

I. Description des corps finis [TaC] - [Pe]

1. Corps premiers
def, $\text{car}(K) = p$ – K fini $\Rightarrow |K| = p^n$
2. Structure des corps finis
Wedderburn – extension, de F_p : degré, base, pol min, etc...
3. Construction
Corps de dec de $X^q - 1 = \sim F_p[X]/(P)$, ex

III. Polynômes sur un corps fini [Dmz]

1. Irreductibilité de Φ_n
irred sur \mathbb{Q} / sur F_p - Φ_{p^r} prod de pol irred
2. Extensions cyclotomiques
def, ex
3. Polynômes irréductibles sur F_p
dec de $X^{p^m} - X$, critère d'irred – nb de pol irred

IV. Applications [Pe]

1. Formes quadratiques sur F_q
def discriminant – classification
2. En arithmétique : carrés mod q
gpe F_q^* - carrés ds F_q , somme de 2 carrés
symbole de Legendre, Th d'Euler, loi de réciprocité
3. En algèbre linéaire : groupe linéaire sur F_p
cardinaux et isom exceptionnels

Biblio :

Perrin
Tauvel (corps et th de Galois)
Demazure

Développements :

13 – Polynômes irréductibles sur F_p
31 – Classification des formes quadratiques sur F_q
33 – Loi de réciprocité quadratique