Préparation à l'Agrégation 2005 UNSA 2004-05

Feuille d'exercices n°7 : CORPS FINIS

I] a) On pose $\mathbb{F}_8 = \frac{\mathbb{F}_2[X]}{(X^3+X+1)} = \mathbb{F}_2[\alpha]$ (α = classe de X). Calculer les racines de X^3+X+1 dans $\mathbb{F}_8$. [Rép : $\alpha, \alpha^2, \alpha^2+\alpha$]

b) Même question pour $\mathbb{F}_8' = \frac{\mathbb{F}_2[X]}{(X^3+X^2+1)} = \mathbb{F}_2[\beta]$ et X^3+X^2+1.
[Rép : $\beta, \beta^2, \beta^2+\beta+1$]

c) Décomposer X^8-X en facteurs irréductibles dans $\mathbb{F}_2[X]$, dans $\mathbb{F}_8[X]$ et dans $\mathbb{F}_8'[X]$

d) Exhiber un isomorphisme de corps $\mathbb{F}_8 \xrightarrow{\sim} \mathbb{F}_8'$

[Rép : $\alpha \longmapsto \beta+1$]

II] Prouver que $\mathbb{F}_{16} = \frac{\mathbb{F}_2[X]}{(X^4+X+1)}$.

$\frac{\mathbb{F}_2[X]}{(X^4+X^2+1)}$ est-il un corps ? et $\frac{\mathbb{F}_2[X]}{(X^3+X^3+1)}$?

III] Prouver que, pour p premier impair,

X^2+1 est irréductible $\Longleftrightarrow p \equiv 1 \pmod 4$ dans $\mathbb{F}_p[X]$

En déduire des constructions de $\mathbb{F}_{25}, \mathbb{F}_{169}, \dots$

[Indic : $(\mathbb{F}_p^*, \cdot) \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$]