Première partie

test

Chapitre 1

rfee

R En utilisant un corps premier, la construction d'un anneau quotient avec un élément irréductible permet de construire de nouveaux corps finis de type $\mathbb{F}_p[X]/m$, différents des corps premiers.

Proposition 1 — L'anneau $(\mathbb{F}_p[X]/m, +, \times)$ est un corps si et seulement si m est irréductible.

V **Vocabulary 1 — Corps de rupture (Splitting Fields)** $\leftrightsquigarrow$ En anglais, les corps $(\mathbb{F}_p[X]/m, +, \times)$ ainsi généré se nomme Splitting Fields, corps de rupture en français.

Théorème 1 — Le cardinal du corps $\mathbb{F}_p[X]/m$ avec $m \in \mathbb{F}_p[X]$ irréductible et $\deg(m) = n$ est p^n .

Démonstration. D'après la relation de congruence et les propriétés de la division euclidienne, $\mathbb{F}_p[X]/m$ est l'ensemble des polynômes à coefficients dans $\mathbb{F}_p$ dont le degré est strictement inférieur à n. Ce sont des polynômes à n coefficients a_i à valeur dans $\mathbb{F}_p$. Pour chaque a_i, on a donc p valeurs possibles. D'où le résultat. ■