

## EXERCICES DE RÉVISION

Dans toute cette feuille,  $p$  désigne un nombre premier et  $q := p^\alpha$  avec  $\alpha \geq 1$ .

1. Soit  $\mathbb{A}$  un anneau commutatif unitaire intègre de caractéristique  $p$  et soit  $n \geq 1$ .  
Montrer que :

$$\forall x, y \in \mathbb{A}, \quad (x + y)^{p^n} = x^{p^n} + y^{p^n}.$$

Que dire si  $\mathbb{A} = \mathbb{F}_{p^n}$  ?

2. On note  $(\mathbb{F}_q^*)^2$  l'ensemble des éléments de  $\mathbb{F}_q^*$  qui sont des carrés dans ce corps.
  - (a) Si  $p = 2$ , montrer que  $(\mathbb{F}_q^*)^2 = \mathbb{F}_q^*$ .
  - (b) Si  $p \neq 2$ , montrer que  $|(\mathbb{F}_q^*)^2| = \frac{q-1}{2}$ .
  - (c) On suppose que  $p$  impair ; montrer que  $a \in \mathbb{F}_q^*$  est un carré si et seulement si  $a^{\frac{q-1}{2}} = 1$ . En déduire que dans ce cas  $\mathbb{F}_p[X]/(X^2 + 1)$  est un corps si et seulement si  $p \equiv 3[4]$ .
3. Quels sont les sous-corps de  $\mathbb{F}_{4096}$  ? Décrire les injections existant entre ces derniers.
4. Déterminer une C.N.S sur  $n$  pour que l'idéal  $(n, X)$  soit premier dans  $\mathbb{Z}[X]$ .  
Même question concernant la maximalité.
5. Le polynôme  $X^4 + X^2 + 1$  est-il irréductible sur  $\mathbb{F}_2$  ?
6. Dresser la liste des polynômes irréductibles de degré 3 sur  $\mathbb{F}_3$ .
7. Montrer que l'anneau  $\mathbb{F}_2[X]/(X^2 + X + 1)$  est un corps isomorphe à  $\mathbb{F}_4$ . En déduire les tables d'addition et de multiplication ainsi qu'une  $\mathbb{F}_2$ -base de ce dernier corps. Quels sont les générateurs de  $\mathbb{F}_4^\times$  ?
8. Que dire de  $\mathbb{F}_p[X]/(X^2 + X + 1)$  avec  $p = 3, 5$  ?
9. Justifier pourquoi  $\mathbb{F}_3[X]/(X^2 + 2X + 2)$  et  $\mathbb{F}_3[X]/(X^2 + 1)$  sont des corps isomorphes. Expliciter un isomorphisme entre ces deux corps.

**Problème 1 : polynômes irréductibles dans  $\mathbb{F}_q[X]$ .** Pour  $n \geq 1$  on note  $A(n, q)$  l'ensemble des polynômes de degré  $n$  irréductibles sur  $\mathbb{F}_q$ . Fixons un entier  $n \geq 1$ .

1. Soit  $d|n$  et soit  $P \in A(d, q)$  ; montrer que  $\mathbb{F}_q[X]/(P)$  est un corps isomorphe à  $\mathbb{F}_{q^d}$ . En déduire que si  $x$  est la classe de  $X$  dans  $\mathbb{F}_q[X]/(P)$  on a  $x^{q^n} = x$ .
2. Montrer que l'on a dans  $\mathbb{F}_{q^n}[X]$  l'égalité suivante :

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d, q)} P.$$

3. Montrer que l'on a l'équivalent suivant :

$$\text{Card}(A(n, q)) \sim_{n \rightarrow \infty} \frac{q^n}{n}.$$

*Indication : on pourra faire usage de la formule d'inversion de Möbius.*

**Problème 2 : le théorème de Chevalley–Warning.** Le but de ce problème est de prouver le résultat suivant.

**Theorem** (Chevalley–Warning). *Soit  $A$  un ensemble fini et soit  $(f_\alpha)_{\alpha \in A}$  une famille de polynômes à  $n$  indéterminées ( $n \geq 1$ ) sur  $\mathbb{F}_q$  tels que :*

$$\sum_{\alpha \in A} \deg(f_\alpha) < n .$$

*On considère la courbe algébrique  $V$  définie par les  $f_\alpha$ , à savoir*

$$V := \{\underline{x} \in \mathbb{F}_q^n \mid \forall \alpha \in A, f_\alpha(\underline{x}) = 0\} \subset \mathbb{F}_q^n .$$

*Alors le cardinal de  $V$  est congru à 0 modulo  $p$ .*

1. Montrer que la fonction caractéristique de  $V$   $\chi_V : \mathbb{F}_q^n \rightarrow \{0, 1\}$  est égale à

$$\underline{x} \mapsto \prod_{\alpha \in A} (1 - f_\alpha(\underline{x})^{q-1}) .$$

2. Pour  $u \in \mathbb{N}$  on pose :

$$S(X^u) := \sum_{x \in \mathbb{F}_q} x^u .$$

Montrer que  $S(X^u) = -1$  si  $u \geq 1$  et  $q-1 \mid u$  et que  $S(X^u) = 0$  sinon.

3. Pour  $f \in \mathbb{F}_q[X_1, \dots, X_n]$  on pose :

$$S(f) := \sum_{x \in \mathbb{F}_q^n} f(\underline{x}) .$$

Montrer que  $S(\chi_V) = 0$  dans  $\mathbb{F}_q$ . *Indication : faire le lien avec la question précédente ...*

4. Conclure.