

**Exercices du cours de Théorie de l'Information et Codage**  
cours 9 du 3 mai 2011.

1. Soit  $F$  est une extension finie de  $F(p)$  qui contient tous les zéros de  $X^{p^m} - X$ . Montrer (i) que  $X^{p^m} - X$  a tous ses zéros distincts dans  $F$ ; (ii) directement que ces zéros forment un corps.
2. Soit  $G$  un groupe commutatif contenant des éléments  $g$  et  $h$  d'ordres  $r$  et  $s$  respectivement. (i) Montrer que si  $g^n = 1$  alors  $r|n$ . (ii) Montrer que si  $r \wedge s = 1$  alors  $gh$  a pour ordre  $rs$ . (iii) Montrer que si  $r = r_1 r_2$  alors  $g_1^{r_1}$  a pour ordre  $r_2$ .
3. (i) Montrer que dans tout corps:

$$X^s - 1 | X^r - 1 \Leftrightarrow s|r.$$

(ii) Montrer que  $p.g.c.d.\{X^r - 1, X^s - 1\} = X^d - 1$  avec  $d = p.g.c.d.\{r, s\}$ .

4. Montrer la propriété (M7) du cours (Rappel: pour  $\alpha \in F(p^m)$ , on a  $\alpha \in F(p)$  ssi  $\alpha^p = \alpha$ ).