Exercices du cours de Théorie de l'Information et Codage

cours 9 et 10 des 13 avril et 4 mai 2010.

1. Soit G un groupe commutatif, g et h deux éléments d'ordres respectifs r et s. Montrer que

   (i) si $g^n = 1$ alors $r|n$.

   (ii) si r et s sont premiers entre eux, alors l'ordre de gh est rs.

   (iii) si $r = r_1 r_2$ alors g^{r_1} a pour ordre r_2.

2. Soit F une extension finie du corps $GF(p)$ qui contient tous les zéros de $x^{p^m} - x$.

   (i) Montrer que $x^{p^m} - x$ a des zéros distincts dans F. (On pourra considérer le polynôme dérivé).

   (ii) Montrer directment que ces zéros forment un corps.

3. Montrer que si n, r, s sont des entiers avec $n \geq 2$, $r \geq 1$ et $s \geq 1$ alors $n^s - 1|n^r - 1$ ssi $s|r$. Montrer que dans tout corps, $x^s - 1|x^r - 1$ ssi $s|r$. En déduire le Théorème suivant:

   (i) $GF(p^r)$ contient un corps (isomorphe à) $GF(p^s)$ ssi s divise r.

   (ii) Si $\beta \in GF(p^r)$ alors $\beta \in GF(p^s)$ ssi $\beta^{p^s} = \beta$.

4. Montrer que les coefficients du polynôme défini dans la propriété (M7) par $\prod_{j \in C_s}(x - \alpha^j)$ sont dans $GF(p)$ en déduire une preuve de (M7).

5. Montrer que $\pi(x) = x^4 + x^3 + x^2 + x + 1$ est irreductible sur $GF(2)$ (donc peut être utilisé pour générer $GF(2^4)$) mais n'est pas primitif.