Solutions des 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.

   - Si $(X-\alpha)^k$ divise un polynôme $f(X)$ alors $(X-\alpha)^{k-1}$ divise le polynôme dérivé $f'(X)$. Ici, le polynôme dérivé de $X^{p^m} - X$ est -1 donc (i) est vrai. (ii) se vérifie facilement.

2. Soit G un groupe commutatif contant 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 a pour ordre r_2.

   (i) On écrit $n = qr + s$ avec $s < r$ de telle sorte que $g^n = g^s = 1$ donc $s = 0$.

   (ii) On a clairement $(gh)^{rs} = 1$ donc l'ordre n de gh est $n \leq rs$. Si $n < rs$ alors en écrivant $rs = qn + t$ avec $t < n$, on obtient $(gh)^t = 1$ donc $t = 0$ mais $r \wedge s = 1$ donc $q = 1$.

   (iii) Si n est l'ordre de g^{r_1} alors on doit avoir $nr_1 \geq r$, c'est à dire $n \geq r_2$, l'inégalité dans le sens opposé est triviale.

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 $d = p.g.c.d.\{r, s\}$.

   (i) Il suffit d'observer que si $r = ks + t$ avec $0 \leq t < s$, on obtient par division Euclidienne de $X^r - 1$ par $X^s - 1$:

$$X^r - 1 = (X^s - 1)(X^{(k-1)s+t} + \cdots + X^t) + X^t - 1$$

   (ii) En supposant $s \geq r$, on écrit $s = qr + t$ avec $t < r$, on a

$$X^s - 1 = (X^r - 1)(X^{s-r} + \cdots + X^{s-qr}) + X^t - 1,$$

   donc $p.g.c.d.\{X^r - 1, X^s - 1\} = p.g.c.d.\{X^r - 1, X^t - 1\}$ et l'algorithme d'Euclide permet de conclure.

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

   - Il suffit de montrer que pour les fonctions élémentaires symétriques des α^j, j étant dans une classe cyclotomique, sont dans $F(p)$. La classe cyclotomique contenant s est $C_s = \{s, ps, \ldots p^{m_s - 1}s\}$ avec m_s le plus petit entier tel que $p^{m_s - 1}s = s \mod [p^m - 1]$. On a donc

$$\left(\sum_{j \in C_s} \alpha^j\right)^p = \sum_{j \in C_s} \alpha^{pj} = \sum_{j \in C_s} \alpha^j.$$

   Un calcul similaire pour les autres fonctions élémentaires permet de conclure.