Solutions des 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.

   - la division Euclidienne de n par r donne: $n = qr + t$ avec $0 \leq t \leq r-1$. On a alors $g^{qr+t} = g^t = 1$ donc $t = 0$.
   - Soit t l'ordre de gh. $(gh)^t = 1$, donc $g^t = h^{-t}$, $g^{st} = h^{-st} = 1$ et $h^{-rt} = g^{rt} = 1$. Comme $g^{st} = 1$, on a $r|st$ donc $r|t$. De même $s|t$ donc $rs|t$ et clairement $(gh)^{rs} = 1$ ce qui conclut la preuve de (ii).
   - Soit t l'ordre de g^{r_1}. On a $t|r_2$ et $r \leq r_1 t$ donc $t = r_2$.

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.

   - Rappel si $f(x) = \sum_{i=0}^{n} a_i x^i$ alors $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. Si $f \in F[X]$, un élément $a \in F$ est racine multiple de f ssi a est une racine et $f'(a) = 0$. En effet, si a est une racine, on peut écrire: $f(x) = (x-a)^m g(x)$ avec g premier avec $x - a$. On a alors

     $$f'(x) = (x-a)^m g'(x) + m(x-a)^{m-1} g(x).$$

     Si $m > 1$ alors $f'(a) = 0$. Inversement si $m = 1$ alors $f'(x) = (x-a)g'(x) + g(x)$ et donc $f'(a) = g(a) \neq 0$. Maintenant pour $f(x) = x^{p^m} - x$, on a $f'(x) = -1$ car F est de caractéristique p.
   - Vérifications aisées. Ex: stabilité pour l'addition: $f(\alpha + \beta) = (\alpha + \beta)^{p^m} - (\alpha + \beta) = f(\alpha) + f(\beta) = 0$.

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 $\beta^{p^s} = \beta$.

   - On écrit $r = qs + t$ avec $0 \leq t < s$. Alors

     $$\frac{n^r - 1}{n^s - 1} = n^t \frac{n^{qs} - 1}{n^s - 1} + \frac{n^t - 1}{n^s - 1}.$$

     Comme $n^{qs} - 1$ est toujours divisible par $n^s - 1$, le dernier terme est inférieur à 1 et donc est entier ssi $t = 0$.

- De manière similaire:
$$\frac{x^r-1}{x^s-1} = x^t\frac{x^{qs}-1}{x^s-1} + \frac{x^t-1}{x^s-1},$$
et $x^{qs}-1$ est toujours divisible par x^s-1.
- (i) Si $s|r$, alors par l'exercice précédent, $GF(p^r)$ contient un corps isomorphe à $GF(p^s)$ car $x^{p^s-1}-1|x^{p^r-1}-1$. Inversement, soit β un élément primitif de $GF(p^s)$. Alors
$$\beta^{p^s-1} = 1,\ \beta^{p^r-1} = 1.$$
Donc $p^s-1|p^r-1$ et $s|r$.
- (ii) découle directement du théorème de Fermat.

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).

- Soit $e_k(x_1,\ldots,x_n) = \sum_{1\le j_1\le j_2\cdots\le j_k\le n} x_{j_1}x_{j_2}\ldots x_{j_k}$ de telle sorte que le k-ème coefficient de $\prod_{j\in C_s}(x-\alpha^j)$ est $e_k(\alpha^j)$. D'après l'exercice précédent, on a $e_k(\alpha^j)\in GF(p)$ ssi $e_k(\alpha^j)^p = e_k(\alpha^j)$. Cette dernière propriété découle de la définition de la classe cyclotomique C_s.
- la propriété (M7) découle alors de (M2).

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.

- Soit α la racine de π. Alors on a $\alpha^5 = 1$.