TD Corps finis 29 Septembre et 10 Octobre 2015

1. Montrer les isomorphismes suivants et donner un générateur du groupe des inversibles des corps en question :
   (a) $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$;
   (b) $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2+X-1)$.
2. Soit k un corps fini et soit K une extension finie de k. Montrer qu'il existe $\alpha \in K$ tel que $K = k[\alpha]$.
3. (a) Calculer le pgcd de 9 et 6 et $u, v \in \mathbb{Z}$ tels que $pgcd(9,6) = 9u + 6v$.
   (b) Calculer le pgcd de $P = 2X^4 - 3X^2 + 1$ et $Q = X^3 + X^2 - X - 1$ dans $\mathbb{Q}[X]$ et $U, V \in \mathbb{Q}[X]$ tels que $pgcd(P,Q) = UP + VQ$.
   (c) En appliquant l'algorithme d'Euclide étendu, calculer l'inverse de $X^3 - X + 1$ dans $\mathbb{Q}[X]/(X^2+X+1)$.
4. Montrer que $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$.
   (a) Soit $\alpha = \bar{X}$ la classe de X dans $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$. Montrer que α est un élément primitif de $\mathbb{F}_8$: i.e. α est un générateur du groupe $\mathbb{F}_8^*$.
   (b) Écrire la table de logarithmes de base α : pour tout $a \in \mathbb{F}_8^*$ déterminer a tel que $a = \alpha^i$.
   (c) Soit $g \in \mathbb{F}_8[X]$ défini par $g = (X-\alpha)(X-\alpha^2)$. Montrer que $g = X^2 + \alpha^4 X + \alpha^3$.
   (d) Écrire une matrice génératrice du code de Reed-Solomon C de longueur 7 engendré par g.
   (e) Montrer que dans $\mathbb{F}_2[X]$ on a

   $$X^7 - 1 = (X^2 + \alpha^4 X + \alpha^3)(X^5 + \alpha^4 X^4 + X^3 + \alpha^5 X^2 + \alpha^5 X + \alpha^4).$$

   Déterminer le polynôme de contrôle et une matrice de contrôle de C.
   (f) Corriger le mot réçu $\alpha^3\alpha^2\alpha\alpha^4\alpha\alpha^4 1$.
5. Soit $P(X) = X^3 + 3X - 2$ dans $\mathbb{Q}[X]$.
   (a) Montrer que $K = \mathbb{Q}[X]/(P)$ est un corps et que, si x est la classe de X dans K, alors $\{1, x, x^2\}$ est une $\mathbb{Q}$-base de K.
   (b) Exprimer $(2x^2 + x - 3)(3x^2 - 4x + 1)$ et $(x^2 - x + 4)^{-1}$ dans cette base.
6. Montrer que le polynôme $P(X) = X^5 + X^2 + X + 2$ est irréductible sur $\mathbb{Z}$: factoriser $\overline{P}(X)$ dans $\mathbb{F}_2[X]$ (indication : montrer que $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$). En déduire que si P n'est pas irréductible sur $\mathbb{Z}$, alors il a une racine dans $\mathbb{Z}$. Conclure (par exemple, montrer que la reduction de P dans $\mathbb{F}_3[X]$ n'a pas de racines).
7. Soit p un nombre premier. Montrer que $P(X) = X^{p-1} + \ldots + X + 1$ est irréductible sur $\mathbb{Q}$ (Indication : considérer $P(X+1)$).