Corrigé de l'examen du 23 janvier 2006

Exercice 1. —

1. (a) Posons $ab = k\delta$, cela donne $da'b = kd\delta'$, c'est-à-dire $a'b = k\delta'$. On sait que δ' est premier avec a', le résultat découle du lemme de Gauss.

   (b) On a $\delta = d\delta'$, où d divise a et δ' divise b.

2. Avec les notations ci-dessus, si $\delta \in D(ab)$, on a $\delta = \psi(d, \delta')$.
   Réciproquement, si $(u, v) \in D(a) \times D(b)$, il est clair que $\psi(u, v) = uv \in D(ab)$.

3. Soit u et $u' \in D(a)$, et v et $v' \in D(b)$. Si $\operatorname{pgcd}(a, b) = 1$, alors $\operatorname{pgcd}(u, v') = \operatorname{pgcd}(u', v) = 1$. Supposons $\psi(u, v) = \psi(u', v')$, c'est-à-dire $uv = u'v'$, il résulte alors du lemme de Gauss que u divise u' et que u' divise u. Il en résulte que $u = u'$, donc $v = v'$. L'application ψ est injective.
   Réciproquement, si $\operatorname{pgcd}(a, b) = d > 1$, posons $a = da'$ et $b = db'$. Il est clair que $a \neq a'$ et que $\psi(a, b') = \psi(a', b) = da'b'$. L'application ψ n'est pas injective.

4. On a

$$S(a)S(b) = \left(\sum_{u \in D(a)} u\right)\left(\sum_{v \in D(b)} v\right) = \sum_{(u,v) \in D(a) \times D(b)} uv = \sum_{(u,v) \in D(a) \times D(b)} \psi(u, v).$$

   Si l'application ψ est bijective, on a

$$\sum_{(u,v) \in D(a) \times D(b)} \psi(u, v) = \sum_{w \in D(ab)} w = S(ab).$$

5. Pour tout entier positif n, $D(n)$ contient 1 et n, on en déduit $S(n) \geq n + 1$. Si p est premier, ses seuls diviseurs sont 1 et p. Réciproquement, si p n'est pas premier soit δ un diviseur propre de p, alors $S(p) \geq p + 1 + \delta > p + 1$.

6. Il est clair que les entier 2^{k-1} et $2^k - 1$ sont premiers entre eux, il résulte donc de la question 4 que $S(n) = S(2^{k-1})S(2^k - 1)$. Or

   – $D(2^{k-1}) = \{2^i \mid i = 0, 1, \ldots, k-1\}$, on en déduit $S(2^{k-1}) = \sum_{i=0}^{k-1} 2^i = 2^k - 1$.

   – Il résulte ensuite de la question 5 que $S(2^k - 1) = 2^k$ si et seulement si $2^k - 1$ est premier, auquel cas on a $S(n) = (2^k - 1)2^k = 2n$.

7. $2^k - 1$ est premier pour $k = 2$, 3, 5 et 7, ce qui donne les nombres parfaits 6, 28, 496 et 8 128.

Exercice 2. —

1. Le polynôme $P = X^4 + X^3 + 1$, n'ayant pas de racine dans $\mathbb{F}_2$, n'est divisible par aucun polynôme de degré 1 de $\mathbb{F}_2[X]$, donc par aucun polynôme de degré 3 de $\mathbb{F}_2[X]$. D'autre part, P n'est pas divisible par le polynôme $X^2 + X + 1$, seul polynôme irréductible de degré 2 dans $\mathbb{F}_2[X]$. Le polynôme P est donc irréductible dans $\mathbb{F}_2[X]$, ce qui fait que $\mathbb{K}$ est un corps à 16 élément et de caractéristique 2.

2. On a $\alpha^4 = 1 + \alpha^3$, ce qui donne $\alpha^5 = \alpha + \alpha^4 = 1 + \alpha + \alpha^3$.

3. Le groupe $\mathbb{K}^*$ étant d'ordre 15, l'ordre de α ne peut être que 1, 3, 5 ou 15.
   Comme $\mathcal{B} = \{1, \alpha, \alpha^2, \alpha^3\}$ est une base de $\mathbb{K}$, on a $\alpha \neq 1$ $\alpha^3 \neq 1$, et $\alpha^5 = 1 + \alpha + \alpha^3 \neq 1$. Il en résulte que α est d'ordre 15.

4. $(\alpha^{15} = 1) \Longrightarrow (a^3 = 1)$, l'ordre de a divise donc 3, et comme $a \neq 1$, a est d'ordre 3.

5. On sait que $a = 1 + \alpha + \alpha^3$, donc

$$a^2 = (1 + \alpha + \alpha^3)^2 = 1 + \alpha^2 + \alpha^6 = \alpha + \alpha^3 = a + 1.$$

6. Comme pour tout $x \in \mathbb{K}$, on a $x = -x$, le symétrique de tout élément de $\mathbb{L}$ appartient à $\mathbb{L}$, il résulte ensuite de la relation $a^2 = a + 1$ que la somme de deux éléments de $\mathbb{L}$ appartient à $\mathbb{L}$, c'est-à-dire que $\mathbb{L}$ est un sous-groupe additif de $\mathbb{K}$. D'autre part, $\mathbb{L}$ est stable pour la multiplication puisque $a^3 = 1 \in \mathbb{L}$. $\mathbb{L}$ est donc un sous-anneau de $\mathbb{K}$ donc un sous-corps de $\mathbb{K}$.
7. Il est clair que 0 et 1 vérifient la relation $x^4 = x$. D'autre part, $a^3 = 1$, d'où $a^4 = a$ et $a^8 = a^2$, ce qui montre que a et a^2 vérifient la relation $x^4 = x$. On a donc l'inclusion $\mathbb{L} \subseteq \{x \in \mathbb{K} \,|\, x^4 = x\}$. Or les éléments de l'ensemble $\{x \in \mathbb{K} \,|\, x^4 = x\}$ sont les racines dans $\mathbb{K}$ du polynôme $X^4 + X$ de degré 4, on en déduit $\#\{x \in \mathbb{K} \,|\, x^4 = x\} \leq 4$, d'où l'égalité $\mathbb{L} = \{x \in \mathbb{K} \,|\, x^4 = x\}$ puisque $\#\mathbb{L} = 4$.
8. Soit $\mathbb{L}_1$ un sous-corps de $\mathbb{K}$ à 4 éléments, le groupe multiplicatif $\mathbb{L}_1^*$ est d'ordre 3, tous ses éléments vérifient donc la relation $x^3 = 1$, d'où $x^4 = x$. On en déduit $\mathbb{L}_1^* \subseteq \mathbb{L}$, donc $\mathbb{L}_1 \subseteq \mathbb{L}$ puisque $0 \in \mathbb{L}$. L'égalité vient du fait que $\#\mathbb{L}_1 = \#\mathbb{L}$.
9. Soit $\mathbb{K}_1$ un sous-corps de $\mathbb{K}$ à q éléments, avec $2 \leq q < \#\mathbb{K}$.
   On sait que $\mathbb{K}_1$ est de caractéristique 2, donc qu'il existe un entier positif r tel que $q = 2^r$.
   Le groupe multiplicatif $\mathbb{K}_1^*$, d'ordre $2^r - 1$, est un sous-groupe de $\mathbb{K}^*$, ce qui signifie que $2^r - 1$ divise 15, c'est-à-dire que $r = 1$ ou $r = 2$.
   Ainsi tout sous-corps non trivial $\mathbb{K}_1$ de $\mathbb{K}$ est de cardinal 2 ou 4.
   – Si $q = 2$, les éléments de $\mathbb{K}_1$ vérifient la relation $x^2 = x$, donc $\mathbb{K}_1 = \mathbb{F}_2$ (cf. cours).
   – Si $q = 4$, on a vu à la question précédente qu'on a $\mathbb{K}_1 = \mathbb{L}$.

Exercice 3. —

1. Les 4 dernières colonnes de la matrice G_1 sont linéairement indépendantes, la matrice est donc de rang maximum 4. Ce qui implique que ses 4 lignes sont linéairement indépendantes dans $\mathbb{F}_2^7$.
2. (a) Le code C_1 est le sous-espace vectoriel de $\mathbb{F}_2^7$ engendré par les 4 lignes de la matrice G_1, il est donc de longueur 7 et de dimension 4 puisque les 4 lignes de G_1 sont linéairement indépendantes. Il contient donc $2^4 = 16$ mots.
   (b) Le code C_1 n'est pas systématique car ses 4 premières colonnes sont liées dans $\mathbb{F}_2^4$ par la relation linéaire $c_1 + c_2 + c_3 = c_4$.
3. (a) Le code C_2 est systématique car ses 4 premières colonnes sont linéairement indépendantes dans $\mathbb{F}_2^4$.
   (b) La matrice G_2 se déduit de la matrice G_1 par permutation des colonne 4 et 6 et des colonnes 5 et 7.
   (c) Il est facile de vérifier que la matrice H_2 est de rang maximum 3 et que $H_2\, {}^tG_2 = 0$.
   (d) Deux colonnes distinctes de la matrice H_2 sont linéairement indépendantes, donc $d \geq 3$. Les colonnes 1, 2 et 4 de H_2 sont liées, il existe donc un mot de code de poids 3. On en déduit que $d = 3$.
4. Il résulte de la question 3b que la matrice H_1 déduite de H_2 par permutation des colonnes 4 et 6 et des colonnes 5 et 7 est une matrice de contrôle du code C_1.

$$H_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

5. (a) Le syndrome du mot 1110010 est $H_1(1110010) = 111$, troisième colonne de H_1. L'erreur a affecté la troisième lettre, le mot de code envoyé est 1100010.
   (b) Un calcul facile montre que $m = 1100$.