Corrigé du contrôle continu le 13/11/2015

Solution 1 (4 pts) : a) On a $n = 792 = 2^3 \times 3^2 \times 11$, donc

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n) = 2^2 \times 3(3-1) \times (11-1) = 4 \times 6 \times 10 = 240.$$

Par le théorème chinois, $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/2^3\mathbb{Z})^\times \times (\mathbb{Z}/3^2\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times$. Les deux derniers facteurs sont groupes cycliques d'ordres 6 et 10 respectivement, mais le premier ne l'est pas, isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ainsi l'ordre maximal des éléments dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est $\mathrm{ppcm}(2, 6, 10) = 30$.

b) i) Comme $57 \wedge 141 = 3$, on a $(\frac{57}{141}) = 0$.
ii) $(\frac{38}{159}) = (\frac{2}{159})(\frac{19}{159}) = 1 \times (-1) \times (\frac{7}{19}) = (\frac{5}{7}) = (\frac{2}{5}) = -1$.

c) Une base de Γ est $\{(1,1,0), (0,1,1), (0,0,2)\}$, et le covolume est 2.

Barème : a) 1+0.5 ; b) 0.5+1 ; c) 0.5+0.5.

Solution 2 (3 pts) : a) p étant impaire, il s'écrit sous la forme $p = 2k+1$, donc $p^2 - 1 = 4k^2 + 4k = 4k(k+1)$ est un multiple de 8 car $k(k+1)$ est un multiple de 2.

b) Si $\zeta^8 = 1$, alors $\zeta^{p^2-1} = 1$ par a). Donc $\zeta \in \mathbb{F}_{p^2}$.

c) Si $p = 2$, alors $P = X^4 + 1 = X^4 - 1$ est réductible dans $\mathbb{F}_2[X]$.
Supposons p impair. Montrons par l'absurde que P est réductible. S'il était irréductible, alors $K := \mathbb{F}_p[X]/(P)$ serait un corps isomorphe à $\mathbb{F}_{p^4}$; de plus soit ζ la classe de X dans K, alors K est engendré par ζ sur $\mathbb{F}_p$ (en tant qu'un corps). Or, on a vu que $\zeta \in \mathbb{F}_{p^2}$, ça donne une contradiction.

Barème : a) 0.5 ; b) 1 ; c) 1.5.

Solution 3 (6 pts) : a) On vérifie que $P(0) = 1$ et $P(1) = 1$, donc P n'a pas de racine dans $\mathbb{F}_2$, donc il n'a pas de facteur de degré 1. S'il était rédutible, on aurait une décomposition $P = P_1 P_2$ dans $\mathbb{F}_2[X]$ avec $\deg P_1 = \deg P_2 = 2$. Or, l'unique polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$ est $X^2 + X + 1$, qui implique que

$$P(X) = (X^2 + X + 1)^2 = X^4 + X^2 + 1.$$

Ce n'étant pas le cas, on obtient une contradiction. Par conséquent, K est un corps de cardinal $2^{\deg P} = 2^4 = 16$.

b) Une base de K sur $\mathbb{F}_2$ est $\{1, \alpha, \alpha^2, \alpha^3\}$. On a (notons que $\alpha^4 = \alpha + 1$, car $1 = -1$ dans $\mathbb{F}_2$) : $\alpha^5 = \alpha^4\alpha = (\alpha+1)\alpha = \alpha^2 + \alpha$, d'où

$$\alpha^{10} = (\alpha^5)^2 = (\alpha^2 + \alpha)^2 = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1.$$

c) On sait que $K^\times$ est un groupe cyclique d'ordre $16 - 1 = 15$. Donc l'ordre de α, noté $o(\alpha)$, appartient à $\{1, 3, 5, 15\}$. On doit montrer que $o(\alpha) = 15$. Comme le polynôme minimal de α est $P = X^4 + 1$, on a $o(\alpha) \notin \{1, 3\}$. Le calcul dans b) montre que $o(\alpha) \neq 5$, donc $o(\alpha) = 15$.

d) Notons $\Phi_n : K \to K$ l'application $x \mapsto x^{2^n}$. Alors Φ_1 est le morphisme de Frobenius, qui est bien un automorphisme (il est injectif car $x^2 = 0$ implique $x = 0$, donc surjectif car K est de cardinal fini). Comme $\Phi_n = \Phi_1 \circ \cdots \circ \Phi_1$ (n fois), on déduit que Φ_n est aussi un automorphisme. Puisque Φ_4 est l'identité, on voit que le comportement de Φ_n ne dépend que de la congruence $n \mod 4$ (ainsi il suffit donc de traiter le cas $0 \leq n \leq 3$.

On vérifie facilement que $S_n \stackrel{\text{def}}{=} \{x \in K : \Phi_n(x) = x\}$ est un sous-corps de K. D'autre part, le corps de décomposition du polynôme $X^{2^n} - X$ est $\mathbb{F}_{2^n}$, d'où

$$S_n = \mathbb{F}_{2^4} \cap \mathbb{F}_{2^n}.$$

De manière explicite :

1. si $n \equiv 0$ [4], alors $S_n = K$;
2. si $n \equiv 1$ [4], alors $S_n = \mathbb{F}_2 = \{0, \alpha^{15} = 1\}$
3. si $n \equiv 2$ [4], alors $S_n = \mathbb{F}_2^2 = \{0, \alpha^5, \alpha^{10}, \alpha^{15}\}$
4. si $n \equiv 3$ [4], alors $S_n = \mathbb{F}_2 = \{0, \alpha^{15}\}$. (Attention : $\mathbb{F}_{2^3}$ n'est pas contenu dans $\mathbb{F}_{2^4}$!)

Barème : a) 2 ; b) 1 ; c) 1 ; d) 2.

Solution 4 (7 pts) : a) Montrons $\Rightarrow$:

$$1 = x^2 + y^2 = x^2 - \alpha^2 y^2 = (x + \alpha y)(x - \alpha y) = u(x - \alpha y)$$

d'ou $u^{-1} = x - \alpha y$ (et $u \neq 0$). Montrons $\Leftarrow$: réciproquement.

Utilisant $u = x + \alpha y$ et $u^{-1} = x - \alpha y$, on déduit

$$x = \frac{u + u^{-1}}{2}, \quad y = \frac{u - u^{-1}}{2\alpha}.$$

b) Si $p \equiv 1 \pmod 4$, -1 est un carré dans $\mathbb{F}_p$ car $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1$. Donc il existe $\alpha \in \mathbb{F}_p^\times$ tel que $\alpha^2 = -1$. D'après a), il y a une bijection entre les solutions $\{(x, y)\}$ de $(\star)$ et $\{u \in \mathbb{F}_p^\times\}$. Donc le nombre de solutions est le cardinal de $\mathbb{F}_p^\times$, soit $p - 1$.

c) i) Comme $p \equiv 3 \pmod 4$, -1 n'est pas un carré dans $\mathbb{F}_p$, donc $X^2 + 1$ est irréductible dans $\mathbb{F}_p[X]$, donc K est un corps à p^2 éléments. Soit α la classe de X dans K, on a $\alpha^2 = -1$. En écrivant $p = 4k + 3$ avec $k \in \mathbb{N}$, on trouve

$$\alpha^p = \alpha^{4k}\alpha^3 = \alpha^3 = -\alpha.$$

ii) Rappelons d'abord que si $x \in K$, alors $x \in \mathbb{F}_p$ si et seulement si $x^p = x$.

$\Rightarrow$: Supposons $x^p = x, y^p = y$. On calcule : $u^p = (x + \alpha y)^p = x^p + \alpha^p y^p = x - \alpha y = u^{-1}$, où l'on a utilisé l'égalité $\alpha^p = -\alpha$ par i) et le fait que $(a+b)^p = a^p + b^p$ car K est de caractéristique p.

$\Leftarrow$: Supposons $u^p = u^{-1}$. Par conséquent, $u^{-p} = u$. D'après a) : $x = \frac{u+u^{-1}}{2}$, donc

$$x^p = \frac{u^p + u^{-p}}{2^p} = \frac{u^{-1} + u}{2} = x,$$

donc $x \in \mathbb{F}_p$ (on a $2^p = 2$ par le petit théorème de Fermat). La preuve pour y est similaire.

iii) Par ii), il y a une bijection entre les solutions de $(\star)$ avec le sous-ensemble de K :

$$\{u \in K^\times : u^{p+1} = 1\}.$$

Comme $K^\times$ est un groupe cyclique d'ordre $p^2 - 1$, ce dernier ensemble (en fait sous-groupe de $K^\times$) est de cardinal $p + 1$.

d) Pour $p = 7$ qui est congru à 3 modulo 4, il y a $7 + 1 = 8$ solutions pour $(\star)$. En listant x^2 pour tout $x \in \mathbb{F}_7$, on trouve que les solutions sont :

$$\{(0, \pm 1), (\pm 1, 0), (\pm 2, \pm 2)\}.$$

Pour 13, il y a $13 - 1 = 12$ solutions pour $(\star)$, qui sont

$$\{(0, \pm 1), (\pm 1, 0), (\pm 2, \pm 6), (\pm 6, \pm 2)\}.$$

Barème : a) 1.5 ; b) 1 ; c-i) 1.5 ; c-ii) 1 ; c-iii) 1 ; d) 1.