Université de Bretagne Occidentale
UFR Sciences et Techniques
LICENCE DE MATHEMATIQUES

ARITHMETIQUE ET APPLICATIONS, COMBINATOIRE ET GRAPHES

Contrôle continu, le 16 avril 2013, 13h30–14h00

CORRIGE

1a. Comme $2^1, 2^2 \neq 1$ et $2^3 = 1$ dans $\mathbb{F}_7^\star$, $\delta = 2$ convient.

1b. D'après le Théorème de Lagrange, l'ordre d'un élément d'un groupe divise le cardinal de ce groupe. Comme $\mathbb{F}_7^\star$ est de cardinal 6 et 4 ne divise pas 6, le groupe $\mathbb{F}_7^\star$ ne contient pas d'élément d'ordre 4.

1c. Comme X^2+1 est de degré 2, il suffit de montrer que ce polynôme ne possède aucune racine dans $\mathbb{F}_7$. Or, une racine α de X^2+1 dans $\mathbb{F}_7$ serait un élément avec la propriété que $\alpha^2 = -1$. Une telle racine serait donc d'ordre 4, ce qui est exclu par le 1b ci-dessus.

1d. D'après la division euclidienne dans $\mathbb{F}_7[X]$ par X^2+1, le corps K est un espace vectoriel sur $\mathbb{F}_7$ de base $1, \alpha$. Il est donc de dimension 2 sur $\mathbb{F}_7$. Un tel espace vectoriel est isomorphe à l'espace vectoriel $\mathbb{F}_7^2$. Ce dernier possède $7 \times 7 = 49$ éléments. Par conséquent le cardinal de K est égal à 49.

1e. Dans K on a $\alpha \neq 1$, $\alpha^2 = -1 \neq 1$, $\alpha^3 = -\alpha \neq 1$ et $\alpha^4 = 1$. Du coup, α est bien d'ordre 4 dans $K^\star$.

1f. On cherche $a, b \in \mathbb{F}_7$ tels que $(a\alpha + b)^2 = \alpha$. Supposons donc que $(a\alpha+b)^2 = \alpha$. Comme $(a\alpha+b)^2 = 2ab\alpha + (b^2 - a^2)$ et comme $1, \alpha$ est une $\mathbb{F}_7$-base de K, on obtient $2ab = 1$ et $b^2 - a^2 = 0$. La dernière équation implique que $b = \pm a$. Substituer dans la première donne $\pm 2a^2 = 1$, i.e., $a^2 = \pm 4$. Une solution est donc $a = b = 2$. Par conséquent, $\beta = 2\alpha + 2$ convient.

1g. Dans K on a $\beta \neq 1$, car la famille $1, \alpha$ est libre, $\beta^2 = \alpha \neq 1$, $\beta^3 = \alpha\beta = 2\alpha - 2 \neq 1$, $\beta^4 = \alpha^2 = -1$, $\beta^5 = -\beta = -2\alpha - 2 \neq 1$, $\beta^6 = \alpha^3 \neq 1$, $\beta^7 = -2\alpha + 2 \neq 1$, ce qui montre que l'ordre de β est au moins 8. Or, $\beta^8 = \alpha^4 = 1$ d'après le 1e. Cela montre que β est d'ordre 8 dans $K^\star$.

1h. Comme $\beta = 2\alpha + 2$ et $\beta^2 = \alpha$, on a

$$\beta^2 + 3\beta + 1 = \alpha + 6\alpha + 6 + 1 = 0$$

dans K. Le polynôme $P = X^2 + 3X + 1$ dans $\mathbb{F}_7[X]$ annule donc β. Comme $\beta \notin \mathbb{F}_7$, aucun polynôme de degré 1 dans $\mathbb{F}_7[X]$ n'annule β. Il s'ensuit que P est le polynôme minimal de β sur $\mathbb{F}_7$.

1i. Le sous-corps $\mathbb{F}_7[\beta]$ de K est une extension de $\mathbb{F}_7$ de degré $\deg(P) = 2$, où P est le polynôme minimal de β sur $\mathbb{F}_7$ du 1h ci-dessus. Le corps $\mathbb{F}_7[\beta]$ contient donc 49 éléments, autant que K d'après le 1d. Il s'ensuit que $\mathbb{F}_7[\beta] = K$.

1j. On cherche $a, b \in \mathbb{F}_7$ tels que $(a\beta + b)^2 = \beta$. Supposons donc que $(a\beta + b)^2 = \beta$. Comme

$$(a\beta + b)^2 = a^2\beta^2 + 2ab\beta + b^2 = a^2(-3\beta - 1) + 2ab\beta + b^2 = \\ (2ab - 3a^2)\beta + (b^2 - a^2),$$

on obtient $2ab - 3a^2 = 1$ et $b^2 - a^2 = 0$, car $1, \beta$ est une $\mathbb{F}_7$-base de K d'après les 1h et 1i. On en déduit que $b = \pm a$. Du coup, $\pm 2a^2 - 3a^2 = 1$ ou encore $(\pm 2 - 3)a^2 = 1$. On a vu que $\mathbb{F}_7$ ne contient pas une racine carrée de -1. On a donc forcément $(-2 - 3)a^2 = 1$, i.e., $a^2 = 4$. Une solution est donc $a = 2$, $b = -2$, et $\gamma = 2\beta - 2$ convient.

1k. On pourrait procéder comme dans le 1g ci-dessus, mais on préfère recourrir à un résultat général :

Proposition. Soit G un groupe et $x \in G$ un élément d'orde fini. Soit n l'ordre de x et supposons qu'il existe $y \in G$ tel que $y^k = x$ où $k \in \mathbb{N}$. Si tout nombre premier divisant k divise n, alors l'ordre de y est égal à kn.

Démonstration. Soit $f\colon \mathbb{Z} \to G$ le morphisme de groupes déterminé par $f(1) = y$. Comme $y^{kn} = (y^k)^n = x^n = e$, y est d'ordre fini dans G. Soit $\ell \in \mathbb{N}$ l'ordre de y. On a $\ker(f) = \ell\mathbb{Z}$. Soit g la restriction de f au sous-groupe $k\mathbb{Z}$ de $\mathbb{Z}$. Comme $g(k) = f(k) = y^k = x$ et x est d'ordre n, on a $\ker(g) = nk\mathbb{Z}$. Du coup, $\ell\mathbb{Z} \cap k\mathbb{Z} = \ker(f) \cap k\mathbb{Z} = \ker(g) = nk\mathbb{Z}$. Cela veut dire que $nk = \operatorname{ppcm}(\ell, k)$. Montrons que $\ell = nk$. On le fait en montrant que ℓ et nk ont la même décomposition en facteurs premiers. Soient $p_1, \ldots, p_m$ les nombres premiers divisant k, ℓ ou n. On a

$$k = \prod_{i=1}^{m} p_i^{e_i}, \quad \ell = \prod_{i=1}^{m} p_i^{f_i}, \quad \text{et} \quad n = \prod_{i=1}^{m} p_i^{g_i},$$

où $e_i, f_i, g_i \in \mathbb{N}$. On a donc

$$\prod_{i=1}^{m} p_i^{\max\{e_i, f_i\}} = \operatorname{ppcm}(\ell, k) = nk = \prod_{i=1}^{m} p_i^{e_i + g_i}.$$

D'où $\max\{e_i, f_i\} = e_i + g_i$ pour tout i. D'après l'hypothèse portant sur k, si $e_i \neq 0$, on a $g_i \neq 0$. Du coup, on a $e_i + g_i > e_i$ lorsque $e_i \neq 0$, et donc $f_i = e_i + g_i$

lorsque $e_i \neq 0$. Quand $e_i = 0$, on a également $f_i = \max\{e_i, f_i\} = e_i + g_i$. Ce la montre que $f_i = e_i + g_i$ pour tout i. Par conséquent,

$$\ell = \prod_{i=1}^{m} p_i^{f_i} = \prod_{i=1}^{m} p_i^{e_i+g_i} = kn,$$

comme il fallait démontrer.

Remarque. La condition sur k est indispensable ; si on prend $n = 12$, $k = 10$ et $\ell = 24$, on a bien $\mathrm{ppcm}(\ell, k) = nk$, mais $\ell \neq nk = 120$. Du coup, si on prend pour G le groupe additif $\mathbb{Z}/120\mathbb{Z}$, et on pose $y = 5$ et $x = 50$, l'ordre de x est bien égal à 12, on a $10y = x$, mais l'ordre de y n'est pas égal à 120 puisque $24y = 0$ dans G.

On applique la proposition ici à $G = K^\star$, $x = \beta$, $y = \gamma$. On a $n = 8$, d'après le 1g, et on prend $k = 2$. Comme tout diviseur premier de k divise n, la proposition précédente s'applique et γ est d'ordre 16.

1l. D'après le 1k, γ est d'ordre 16. D'après le 1a, δ est d'ordre 3. Comme 3 et 16 sont premiers entre eux, le produit $\delta\gamma$ est d'ordre 48 dans $K^\star$.