Commentaires sur le sujet MG07

Parties I et III

Salim Rostam et Harold Favereau

Avant-propos

— Il faut mettre en confiance le correcteur ! Comme il était explicitement demandé, il faut *très bien* soigner la rédaction des premières questions (rédiger les récurrences, donner précisément tous les arguments importants, s'appliquer sur la présentation, etc.). Dans la suite on peut se permettre plus de libertés. C'est particulièrement vrai pour la toute première question (nous y reviendrons).

— Je cite le rapport du jury :

  — Dans la partie I, il est utile de rappeler aux candidats que l'on attend d'eux une démonstration précise, même lorsqu'il suffit de faire une récurrence « évidente » : il est tout aussi rapide et beaucoup plus rigoureux de poser précisément la récurrence que de faire un vague discours sur la récurrence que l'on pourrait faire. L'algorithme demandé est souvent très mal décrit. On attendait la description précise des initialisations de variables et des structures de contrôles utilisées ; il est par contre mal venu de s'encombrer de déclarations d'entrées-sorties, d'appels de bibliothèques… surtout lorsqu'ils sont liés à un langage particulier.

  — La partie III s'est révélée extrêmement discriminante. [Elle] a été la moins bien traitée en général et n'a souvent pas été abordée. $\mathbb{F}_{16}$ a été défini de façon fantaisiste : $\mathbb{Z}/16\mathbb{Z}$ ou $(\mathbb{Z}/17\mathbb{Z})^\times$ entre autres.

Partie I

1. C'est la première question du sujet, facile, il ne faut donc pas la rater. Il ne faut pas hésiter à en faire un peu trop, sans toutefois redémontrer les choses au programme. En l'occurence, on pouvait invoquer le théorème de Lagrange pour dire que l'ordre k de a divise le cardinal N du groupe, donc avec $m \coloneqq \frac{N}{k} \in \mathbb{N}^*$ on a $a^N = (a^k)^m = 1^m = 1$.

2. C'était l'algorithme d'exponentiation rapide : pour calculer g^m on calcule $\left(g^{m'/2}\right)^2$ si $m = 2m'$ est pair et $\left(g^{m'/2}\right)^2 g$ si $m = 2m' + 1$ est impair. Cela permet de vérifier que la complexité que l'on retrouve pour le b) est bien logarithmique en N.

3. La fonction indicatrice d'Euler est au programme, en particulier on peut utiliser le fait que si m et n sont premiers entre eux alors $\varphi(mn) = \varphi(m)\varphi(n)$. Rappelons que cette égalité découle du théorème chinois dans lequel on regarde les éléments inversibles.

Partie III

1.a) Il est préférable d'exhiber un polynôme irréductible de degré 4 sur $\mathbb{F}_2$, que l'on obtient par exemple en regardant la suite des questions. D'où l'importance, par ailleurs, de lire l'intégralité du sujet avant de commencer !

1.b) Si ω désigne l'image de X dans $\mathbb{F}_{16} \simeq \mathbb{F}_2[X]/(X^4+X^3+1)$, alors $(1,\omega,\omega^2,\omega^3)$ est une $\mathbb{F}_2$-base de $\mathbb{F}_{16}$, en particulier $\omega \neq 1$. Ainsi, puisque $\omega \in \mathbb{F}_{16}^* \setminus \{1\}$, son ordre est $3, 5$ ou 15. On élimine les deux premiers cas en jouant avec la relation $\omega^4+\omega^3+1=0$ et en utilisant la $\mathbb{F}_2$-base précédente.

1.c) Une chose que l'on remarque est que chaque terme est le carré du précédent. Puisque l'on est en caractéristique 2, ça doit tiquer. Et en effet, on peut utiliser le fait que

$$\begin{array}{ccc} \mathbb{F}_{16} & \longrightarrow & \mathbb{F}_{16} \\ x & \longmapsto & x^2 \end{array},$$

est un morphisme de corps (le morphisme de Frobenius). En particulier, pour tout $a, b \in \mathbb{F}_{16}$ on a $(a+b)^2 = a^2+b^2$, mais aussi

$$(a+b+c)^2 = a^2+b^2+c^2, \tag{$\dagger$}$$

si $a, b, c \in \mathbb{F}_{16}$! On obtient donc directement que ω^2, ω^4 et ω^8 sont également racines de X^4+X^3+1 dans $\mathbb{F}_{16}$, et finalement on a toutes les racines puisqu'elles sont distinctes (on a montré en 1.b) que ω est d'ordre 15).

L'égalité ($\dagger$) se généralise.

Lemme. *Soit p un nombre premier et soit $Q \in \mathbb{F}_p[X]$. Alors $Q(X)^p = Q(X^p)$.*

Démonstration. On utilise le morphisme de Frobenius et le fait que $x^p = x$ pour tout $x \in \mathbb{F}_p$. □

Ainsi, si $\mathbb{F}_q \simeq \mathbb{F}_p(\zeta)$ et si Q est le polynôme minimal de ζ sur $\mathbb{F}_p$, tous les ζ^{p^k} pour $k \in \{0, \dots, d-1\}$ sont racines de Q, où $d \coloneqq \deg Q$. On a même mieux.

Proposition. *Les racines de Q sur $\mathbb{F}_q$ sont* exactement *les ζ^{p^k} pour $k \in \{0, \dots, d-1\}$.*

Démonstration. Par ce qui précède, il suffit de montrer que si $k \neq k' \in \{0, \dots, d-1\}$ alors $\zeta^{p^k} \neq \zeta^{p^{k'}}$. Supposons que $k < k'$ et que $\zeta^{p^k} = \zeta^{p^{k'}}$. En posant $\xi \coloneqq \zeta^{p^k}$ on a donc $\xi = \xi^{p^{k'-k}}$ donc $\xi \in \mathbb{F}_{p^{k'-k}}$. Mais c'est absurde puisque le polynôme minimal de ξ sur $\mathbb{F}_p$ est Q (on a vu que ξ est racine de Q et $Q \in \mathbb{F}_p[X]$ est irréductible par hypothèse) qui est de degré $d > k'-k$. □

Remarque. On peut aussi utiliser la réciproque du Lemme : si q est une puissance de p et si $Q \in \mathbb{F}_q[X]$ vérifie $Q(X)^p = Q(X^p)$ alors $Q \in \mathbb{F}_p[X]$. Cela découle simplement du fait que $a \in \mathbb{F}_q$ est dans $\mathbb{F}_p$ si et seulement si $a^p = a$. Ainsi, en posant $\widetilde{Q} \coloneqq \prod_{k=0}^{d-1}(X-\zeta^{p^k})$ on constate, en utilisant le Frobenius et l'égalité $(-1)^p = -1$, que $\widetilde{Q}(X)^p = \prod_{k=0}^{d-1}(X^p-\zeta^{p^{k+1}}) = \prod_{k=0}^{d-1}(X^p-\zeta^{p^k}) = \widetilde{Q}(X^p)$ donc $\widetilde{Q} \in \mathbb{F}_p[X]$. Puisque $\widetilde{Q}$ est unitaire, à coefficients dans $\mathbb{F}_p$, annule ζ et est de degré d, on a $\widetilde{Q} = Q$ et on conclut.

En particulier, on retrouve le fait que le polynôme Q est scindé sur $\mathbb{F}_q$, et donc que tout corps de rupture sur $\mathbb{F}_p$ est un corps de décomposition. **Attention** ! Le résultat précédent n'implique *pas* que ζ est un générateur de $\mathbb{F}_q^\times$.

Exemple. Le polynôme $Q \coloneqq X^2+1 \in \mathbb{F}_3[X]$ est irréductible puisque de degré 2 sans racine ($Q(0)=1$ et $Q(1)=Q(-1)=2$). Or, dans $\mathbb{F}_3[X]/(Q) \simeq \mathbb{F}_9$ l'image i de X vérifie $i^2=-1$ donc $i^4=1$ donc i n'engendre pas $\mathbb{F}_9^* \simeq \mathbb{Z}/8\mathbb{Z}$. Cependant, on a bien $i \neq i^3$ puisque $i^3 = -i \neq i$ (car $i \neq 0$ et la caractéristique est différente de 2).

1.d) C'est toujours la même histoire : il faut choisir entre montrer que c'est une famille libre ou une famille génératrice. Souvent la première solution est la plus facile, mais ici c'était plutôt l'autre. On montre d'abord que 1 est dans l'espace engendré (via la somme des racines de X^4+X^3+1) puis ω^3 via le polynôme minimal, ainsi tous les éléments de la $\mathbb{F}_2$-base $(1,\omega,\omega^2,\omega^3)$ sont dans l'espace engendré et c'est gagné.

2.a) Le cas $a = 0$ n'a que la solution nulle puisque $\mathbb{F}_{16}$ est un corps donc intègre, donc on suppose $a \in \mathbb{F}_{16}^*$. On peut voir ici que ça va être facile de résoudre, puisqu'il s'agit simplement de résoudre $5y = b$ dans $\mathbb{Z}/15\mathbb{Z}$ (où $x = \omega^y$ et $a = \omega^b$). Nécessairement b est un multiple de 5, donc en écrivant $b = 5c$ avec $c \in \mathbb{Z}/15\mathbb{Z}$ on obtient $5y = 5c$ donc $y = c$ modulo 3 (rappelons que $5\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z}$), ce qui donne pour $y \in \mathbb{Z}/15\mathbb{Z}$ les cinq solutions $c, c+3, c+6, c+9$ et $c+12$. Si on retourne dans $\mathbb{F}_{16}^*$, l'équation $x^5 = a$ (avec $a \neq 0$) possède des solutions si et seulement si a est de la forme ω^{5c}, auquel cas les solutions sont $\omega^c, \omega^{c+3}, \omega^{c+6}, \omega^{c+9}$ et ω^{c+12}. Au passage on constate que l'on a bien trouvé cinq solutions, comme le laissait présager le degré de l'équation.

Au passage, on rappelle le résultat suivant.

Proposition. *Si $d \mid n$ et $m = \frac{n}{d}$, il y a dans $\mathbb{Z}/n\mathbb{Z}$ exactement $\varphi(d)$ éléments d'ordre d, qui sont les km pour $k \in \{1, \ldots, d\}$ premier à d.*

Dans le contexte de 2.a), si $a \neq 0, 1$ alors a est d'ordre 3 donc de la forme ω^5 ou $\omega^{2\cdot 5} = \omega^{10}$.

2.b) C'était sans conteste la question la plus difficile. En utilisant les propriétés d'une telle base on montre qu'un tel élément γ est nécessairement d'ordre 5, et par la proposition précédente il y a justement $\varphi(5) = 4$ éléments d'ordre 5 dans $\mathbb{F}_{16}^*$, qui sont les ω^{3k} pour $k \in \{1, \ldots, 4\}$. Si γ est un tel élément, on remarque que $\{\gamma, \gamma^2, \gamma^4, \gamma^8\} = \{\omega^3, \omega^6, \omega^9, \omega^{12}\}$ donc il suffit de remarquer que cette famille est une $\mathbb{F}_2$-base de $\mathbb{F}_{16}$. En particulier, il suffit de considérer le cas $\gamma = \omega^3$, auquel cas $\{\gamma, \gamma^2, \gamma^4, \gamma^8\} = \{\gamma, \gamma^2, \gamma^3, \gamma^4\}$. On pourrait montrer que la famille est libre, mais ça s'annonce fastidieux car il faut calculer beaucoup de relations. On pourrait montrer qu'elle est génératrice en montrant que l'une des deux bases précédentes est engendrée, mais ça ne semble pas évident. En remarquant que $0 = \gamma^5 + 1$ (puisque γ est d'ordre 5) $= (\gamma + 1)(\gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1)$, on montre que $X^4 + X^3 + X^2 + X + 1$ est le polynôme minimal de γ sur $\mathbb{F}_p$. En particulier, ce polynôme est irréductible sur $\mathbb{F}_p$ donc puisque γ est une racine de Q on sait que $(1, \gamma, \gamma^2, \gamma^3)$ est une $\mathbb{F}_p$-base de $\mathbb{F}_q$, donc $(\gamma, \gamma^2, \gamma^3, \gamma^4)$ aussi par le lemme suivant.

Lemme. *Soit K/k une extension finie de corps, soit $(x_1, \ldots, x_n)$ une k-base de K et soit $\lambda \in K^*$. Alors $(\lambda x_1, \ldots, \lambda x_n)$ est une k-base de K.*

Démonstration. La famille est clairement libre sur k et a le bon cardinal donc c'est une base. □