Université Paris 7-Denis Diderot
M1 mathématiques

Algèbre
Année 2007-08
L. Merel - R. Mneinmé

Corrigé de l'EXAMEN du 18 janvier 2008

I

1. D'après le lemme des restes chinois, le groupes $(\mathbf{Z}/63\mathbf{Z})^*$ est isomorphe à $(\mathbf{Z}/7\mathbf{Z})^* \times (\mathbf{Z}/9\mathbf{Z})^*$. Or les deux groupes qui interviennent dans ce produit sont cycliques d'ordre 6 (engendrés par les classes de 3 modulo 7 et de 2 modulo 9 respectivement).
2. Comme 2 et 3 sont des nombres premiers entre eux, on a l'isomorphisme de groupes $\mathbf{Z}/6\mathbf{Z} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ et donc l'isomorphisme de groupe $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. Le groupe $\mathbf{Z}/36\mathbf{Z}$ est cyclique, il ne peut donc être isomorphe à $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$.
3. Comme $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ est un groupe d'ordre $36 = 2^2 3^2$ sa composante p-primaire est réduite à l'élément neutre lorsque $p > 3$. Ses parties 2-primaire et 3-primaire sont isomorphes à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ respectivement d'après la question précédente. Elles ont donc respectivement 4 et 9 éléments.
4. Comme 4 est une puissance de 2, un sous-groupe d'ordre 4 de $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ est égal à sa composante 2-primaire, qui est elle-même contenue dans la partie 2-primaire de $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$.
5. D'après la question précédente, un sous-groupe d'ordre 4 de $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ est contenu dans la partie 2-primaire, qui elle même est d'ordre 4, d'après la question **3**. Donc le seul sous-groupe d'ordre 4 de $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ est sa partie 2-primaire. Puisque les groupes $(\mathbf{Z}/63\mathbf{Z})^*$ et $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ sont isomorphes, $(\mathbf{Z}/63\mathbf{Z})^*$ possède un seul sous-groupe d'ordre 4. Ce sous-groupe H est constitué des classes modulo 63 des entiers 1, -1, 8 et -8.

II

1. On a $\Phi_7(X) = (X^7-1)/(X-1) = X^6+X^5+X^4+X^3+X^2+X+1$ et $\Phi_9 = (X^9-1)/(\Phi_3(X)\Phi_1(X)) = X^6+X^3+1$.
2. On a $X^{n/2}\Phi_n^+(X+1/X) = \prod_k (X^2+1-\zeta X-\zeta^{-1}X) = \prod_k (X-\zeta)(X-\zeta^{-1}) = \Phi_n(X)$. En effet, toute racine primitive n-ème de l'unité s'écrit ζ^k ou ζ^{-k} avec k entier premier à n et $0 < k < n/2$.
3. Utilisons la question précédente. On a $\Phi_7(X) = X^3((X+X^{-1})^3 + (X+X^{-1})^2 - 2(X+X^{-1}) - 1)$ et $\Phi_9(X) = X^3((X+X^{-1})^3 - 3(X+X^{-1}) + 1)$. On en déduit $\Phi_7^+(X) = X^3+X^2-2X-1$ et $\Phi_9^+(X) = X^3-3X+1$.
4. Le polynôme Φ_7^+ est de degré 3. Aucun des trois éléments de $\mathbf{F}_3$ n'en est racine, si bien qu'il est irréductible sur $\mathbf{F}_3$.
5. Tout corps de rupture de Φ_7^+ sur $\mathbf{F}_3$ possède $3^3 = 27$ éléments puisque ce polynôme est irréductible sur $\mathbf{F}_3$ et de degré 3. Comme nous sommes sur un corps fini, ce corps de rupture est aussi un corps de décomposition. Comme il n'y a qu'un seul corps à 27 éléments à isomorphisme près, Φ_7^+ est scindé sur tout corps à 27 élément et donc sur tout corps contenant un corps à 27 éléments.

Réciproquement, si Φ_7^+ est scindé sur un corps k, ce dernier contient un corps de décomposition de Φ_7^+ et donc un corps à 27 éléments.

Un corps fini de caractéristique 3 a un cardinal de la forme 3^n avec n entier ≥ 1. Un tel corps contient un corps à 27 éléments si et seulement si 3 divise n.

Conclusion : Φ_7^+ est scindé sur un corps fini de caractéristique 3 si et seulement si ce corps possède 3^{3m} éléments, avec m entier ≥ 1.

III

1. Montrons la double inclusion entre ces corps. Puisque ζ_{63} est une racine primitive 63-ème de l'unité, ζ_{63}^7 et ζ_{63}^9 sont des racines primitives 9-ème et 7-ème respectivement. On a donc $\mathbf{Q}(\zeta_7, \zeta_9) = \mathbf{Q}(\zeta_{63}^7, \zeta_{63}^9) \subset \mathbf{Q}(\zeta_{63})$. Inversement, comme $\zeta_7\zeta_9$ est une racine primitive 63-ème de l'unité, on a $\mathbf{Q}(\zeta_{63}) = \mathbf{Q}(\zeta_7\zeta_9) \subset \mathbf{Q}(\zeta_7, \zeta_9)$.

Le diagramme exprime les inclusions $\mathbf{Q} \subset \mathbf{Q}(\zeta_{63})$ (de degré $\phi(63) = 36$), $\mathbf{Q} \subset \mathbf{Q}(\zeta_7)$ (de degré $\phi(7) = 6$), $\mathbf{Q} \subset \mathbf{Q}(\zeta_9)$ (de degré $\phi(9) = 6$), $\mathbf{Q}(\zeta_7) \subset \mathbf{Q}(\zeta_{63})$ (de degré $\phi(63)/\phi(7) = 6$) et $\mathbf{Q}(\zeta_9) \subset \mathbf{Q}(\zeta_{63})$ (de degré $\phi(63)/\phi(9) = 6$)

2. Comme $\alpha_n = \zeta_n + \zeta_n^{-1} \in \mathbf{Q}(\zeta_n)$, on a $\mathbf{Q}(\alpha_n) \subset \mathbf{Q}(\zeta_n)$. Comme ζ_n est une racine de l'unité, on a $\zeta_n\bar{\zeta_n} = 1$, si bien que ζ_n^{-1} est le conjugué complexe de ζ_n. C'est pourquoi $\alpha_n \in \mathbf{R}$.
3. Comme $\alpha_n = \zeta_n + \zeta_n^{-1}$, ζ_n est racine du polynôme $X^2 - \alpha_n X + 1 \in \mathbf{Q}(\alpha_n)[X]$. Comme ce dernier polynôme est de degré 2, l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}(\alpha_n)$ est de degré ≤ 2. Elle n'est pas de degré 1 car $\mathbf{Q}(\alpha_n) \subset \mathbf{R}$ et $\zeta_n \notin \mathbf{R}$, si bien que $\mathbf{Q}(\alpha_n) \neq \mathbf{Q}(\zeta_n)$.
4. Les extensions $\mathbf{Q}(\alpha_7)|\mathbf{Q}$ et $\mathbf{Q}(\alpha_9)|\mathbf{Q}$ sont de degré $6/2 = 3$. Les extensions $\mathbf{Q}(\zeta_{63}) = \mathbf{Q}(\zeta_7, \zeta_9)|\mathbf{Q}(\zeta_7, \alpha_9)$ et $\mathbf{Q}(\zeta_7, \alpha_9)|\mathbf{Q}(\alpha_7, \alpha_9)$ sont de degré au plus 2. L'extension $\mathbf{Q}(\zeta_{63})|\mathbf{Q}(\alpha_7, \alpha_9)$ est donc de degré ≤ 4.
5. Comme l'extension $\mathbf{Q}(\zeta_{63})|\mathbf{Q}$ est de degré 36 et que l'extension $\mathbf{Q}(\zeta_{63})|\mathbf{Q}(\alpha_7, \alpha_9)$ est de degré ≤ 4, l'extension $\mathbf{Q}(\alpha_7, \alpha_9)|\mathbf{Q}$ est de degré $\geq 36/4 = 9$. Comme l'extension $\mathbf{Q}(\alpha_7, \alpha_9)|\mathbf{Q}$ est composée de deux extensions de degré 3, elle est de degré ≤ 9. Elle est donc de degré 9.

IV

1. L'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ est galoisienne de groupe de Galois abélien. Comme tout sous-groupe d'un groupe abélien est distingué, tout sous-corps K de $\mathbf{Q}(\zeta_n)$ est une extension galoisienne de $\mathbf{Q}$.
2. C'est un sous-groupe d'ordre 2, puisque l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}(\alpha_n)$ est de degré 2. On peut observer que α_n est invariant par l'image de $-1 \in (\mathbf{Z}/n\mathbf{Z})^*$ dans $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}$ (car cette image envoie ζ_n sur ζ_n^{-1}, et donc laisse fixe $\alpha_n = \zeta_n + \zeta_n^{-1}$). Donc $\mathbf{Q}(\alpha_n)$ est contenu dans le corps des invariants du groupe $\{-1, 1\}$. Comme $\mathbf{Q}(\zeta_n)$ est une extension de degré 2 de chacun de ces deux corps, il s'agit bien du même corps. Le groupe H_n est donc $\{-1, 1\}$.
3. Comme l'extension $\mathbf{Q}(\zeta_{63})|\mathbf{Q}(\alpha_7, \alpha_9)$ est de degré $36/9 = 4$, le sous-groupe cherché est d'ordre 4. C'est donc le groupe H trouvé en **I.5**.
4. Cette extension est galoisienne (voir question **IV.1.**). D'après la théorie de Galois, le groupe de Galois correspondant est isomorphe au groupe quotient $(\mathbf{Z}/63\mathbf{Z})^*/H$. Comme $(\mathbf{Z}/63\mathbf{Z})^*$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ et que H est la partie 2-primaire de ce dernier groupe, le quotient $(\mathbf{Z}/63\mathbf{Z})^*/H$ est isomorphe à $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.
5. On peut prendre par exemple le corps $\mathbf{Q}(\zeta_{21})$, qui est contenu dans $\mathbf{Q}(\zeta_{63})$ puisque $21|63$ et qui est de degré 12, puisque $\phi(21) = 12$. (NB : il y a 4 tels corps, correspondant aux 4 sous-groupes d'indice 12 de $(\mathbf{Z}/63\mathbf{Z})^*$, *i.e.* aux 4 sous-groupes d'ordre 3 de $(\mathbf{Z}/63\mathbf{Z})^*$.)